(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-120736
(P2004-120736A)
(43)公開日　平成16年4月15日(2004.4.15)

| (51)Int.Cl.[7] | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| H04L | 9/08 | H04L | 9/00 | 601B | 5J104 |
| H04L | 9/32 | H04L | 9/00 | 601E | |
| | | H04L | 9/00 | 675B | |

審査請求 未請求　請求項の数 68　OL　（全 52 頁）

(21)出願番号　特願2003-305403(P2003-305403)
(22)出願日　平成15年8月28日(2003.8.28)
(31)優先権主張番号　特願2002-260520(P2002-260520)
(32)優先日　平成14年9月5日(2002.9.5)
(33)優先権主張国　日本国(JP)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100090446
弁理士　中島　司朗
(72)発明者　松崎　なつめ
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　阿部　敬久
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　中野　稔久
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】グループ形成管理システム、グループ管理機器及びメンバー機器

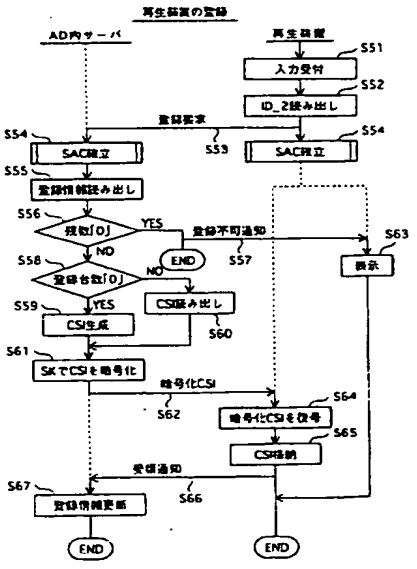
(57)【要約】

【課題】　グループの範囲をより固定的にし、グループ内の機器間ではコンテンツを自由に利用可能なグループ形成管理システムを提供する。

【解決手段】　前記形成管理システムは、グループに固有の共通秘密情報を保持している１個以上の登録済のメンバー機器と、グループへの登録の要求を送信し、共通秘密情報を取得して保持する新規のメンバー機器と、新規のメンバー機器から登録の要求を受け付け、グループに登録されている前記登録済のメンバー機器の台数が、グループに登録可能な最大の台数である制限台数未満の場合、前記新規のメンバー機器を登録し、当該メンバー機器へ前記共通秘密情報を出力するグループ管理機器とから構成される。

また、コンテンツを利用する際には、前記共通認証情報を用いてメンバー機器を認証し、成功した場合にコンテンツを配送するので、前記共通秘密情報を保持しない機器、つまりグループに登録されていないメンバー機器でのコンテンツの利用を防止することが出来る。

【選択図】　図９



【特許請求の範囲】
【請求項１】
グループ形成管理システムであって、
グループに固有の共通秘密情報を保持している１個以上の登録済のメンバー機器と、
グループへの登録の要求を送信し、共通秘密情報を取得して保持する新規のメンバー機器と、
新規のメンバー機器から登録の要求を受け付け、グループに登録されている前記登録済のメンバー機器の台数が、グループに登録可能な最大の台数である制限台数未満の場合、前記新規のメンバー機器を登録し、当該メンバー機器へ前記共通秘密情報を出力するグループ管理機器と
から構成されることを特徴とするグループ形成管理システム。
【請求項２】
グループ形成管理システムであって、
グループへの登録の要求を送信し、グループに固有の共通秘密情報を取得して保持するメンバー機器と、
前記メンバー機器から登録の要求を受け付け、グループに登録されているメンバー機器の台数が、グループに登録可能な最大の台数である制限台数未満の場合、前記メンバー機器を登録し、当該メンバー機器へ前記共通秘密情報を出力するグループ管理機器とから構成され、
初期の状態では、前記グループ管理機器にメンバー機器は登録されていない
ことを特徴とするグループ形成管理システム。
【請求項３】
グループへのメンバー機器の登録を管理するグループ管理機器であって、
前記メンバー機器からグループに登録する旨の登録要求を受け付ける受付手段と、
登録要求が受け付けられると、前記メンバー機器が正当な機器であれば、グループに登録済みのメンバー機器の登録台数が、グループに登録可能な最大の台数である制限台数より少ないか否かを判断し、少ないと判断する場合、前記メンバー機器を登録する判断手段と、
前記制限台数より少ないと判断する場合に、前記メンバー機器へグループに固有の共通秘密情報を出力する通信手段と
から構成されることを特徴とするグループ管理機器。
【請求項４】
前記メンバー機器は、第1初期値を保持し、
前記判断手段は、第2初期値を保持し、前記第2初期値と前記第1初期値とを用いて前記メンバー機器の正当性を認証する認証手段と、
前記認証結果が成功の場合、前記登録台数が前記制限台数より少ないか否かを判断する台数判断手段とを含み、
前記通信手段は、前記共通秘密情報として、当該グループ管理機器により管理されるグループに登録されたことを示す共通秘密情報を出力し、
前記メンバー機器は、前記共通秘密情報を取得して保持し、前記第１初期値の使用を抑制する
ことを特徴とする請求項３のグループ管理機器。
【請求項５】
前記メンバー機器は、前記グループ管理機器に登録されていないことを示す前記第１初期値を保持し、
前記認証手段は、当該グループ管理機器に登録されていないことを示す前記第２初期値と、前記第１初期値とを用いて認証する
ことを特徴とする請求項４のグループ管理機器。
【請求項６】
前記メンバー機器は、当該メンバー機器が何れのグループ管理機器にも登録されていない

ことを示す前記第１初期値を保持し、
　前記認証手段は、前記メンバー機器が何れのグループ管理機器にも登録されていないことを示す前記第２初期値と、前記第１初期値とを用いて認証する
　ことを特徴とする請求項４のグループ管理機器。
【請求項７】
前記グループ管理機器は、更に、
　前記共通秘密情報を生成する生成手段を備え、
　前記通信手段は、生成された前記共通秘密情報を出力する
　ことを特徴とする請求項３のグループ管理機器。
【請求項８】
グループ外の管理装置により前記共通秘密情報を生成され、
　前記判断手段は、グループ外の前記管理装置から前記共通秘密情報を取得し、
　前記通信手段は、取得した前記共通秘密情報を前記メンバー機器へ出力する
　ことを特徴とする請求項３のグループ管理機器。
【請求項９】
前記受付手段は、前記登録要求を受け付けると、グループ外の管理装置に前記登録要求を受け付けた旨を通知し、
　前記グループ外の管理装置は、前記登録台数が、前記グループに登録可能な最大の台数である制限台数より少ないか否かを判断し、
　前記判断手段は、前記登録台数が前記制限台数より少ないか否かを判断する代わりに、前記管理装置から判断結果を受け取り、
　前記通信手段は、前記判断結果が、前記台数より前記制限台数の方が少ないことを示す場合、前記共通秘密情報を出力する
　ことを特徴とする請求項３のグループ管理機器。
【請求項１０】
前記制限台数は、第1制限台数と第2制限台数とから成り、
　前記判断手段は、登録済みのメンバー機器の台数が、前記第1制限台数又は前記第２制限台数より少ないか否かを判断する
　ことを特徴とする請求項２のグループ管理機器。
【請求項１１】
前記第1制限台数は、前記制限台数のうち、当該グループ管理機器に接続可能なメンバー機器の最大の台数であり、前記第２制限台数は、前記制限台数のうち、当該グループ管理機器に接続できないメンバー機器の最大の台数であり、
　前記判断手段は、前記要求元のメンバー機器が当該グループ管理機器に接続可能なメンバー機器である場合、登録済みの接続可能なメンバー機器の台数が、前記第1制限台数より少ないか否かを判断し、
　前記要求元のメンバー機器が当該グループ管理機器に接続できないメンバー機器である場合、登録済みの接続できないメンバー機器の台数が、前記第２制限台数より少ないか否かを判断する
　ことを特徴とする請求項１０のグループ管理機器。
【請求項１２】
前記通信手段は、更に、他のグループ管理機器に、前記メンバー機器を登録可能であるか否かを問い合わせる問合要求を出力し、
　前記他のグループ管理機器は、前記問合要求を受け付け、前記他のグループ管理機器に登録済みのメンバー機器の登録台数が、当該他のグループ管理機器の制限台数より少ないか否かを判断し、少ないと判断する場合、前記メンバー機器を登録し、前記グループ管理機器へ前記共通秘密情報を出力し、
　前記通信手段は、前記他のグループ管理機器から前記共通秘密情報を受信すると、前記メンバー機器へ前記共通秘密情報を出力する
　ことを特徴とする請求項３のグループ管理機器。

【請求項１３】
前記判断手段は、外部からの不正なアクセスに対抗する機能を備え、前記制限台数及び前記共通秘密情報は、外部から読み出し及び書き込みが出来ない領域内に記憶されている
ことを特徴とする請求項３のグループ管理機器。
【請求項１４】
前記判断手段は、前記グループ管理機器に着脱可能な可搬型モジュールから構成されている
ことを特徴とする請求項１３のグループ管理機器。
【請求項１５】
前記判断手段は、前記制限台数から前記登録台数を差し引いた残数を記憶し、前記受付手段が登録要求を受け付けると、前記残数が「０」であるか否かを判断し、
「０」でないと判断する場合、前記通信手段は、前記メンバー機器へ前記共通秘密情報を出力し、
「０」でないと判断する場合、前記判断手段は、前記残数から「１」を減算する
ことを特徴とする請求項３のグループ管理機器。
【請求項１６】
前記メンバー機器に対して前記共通秘密情報が出力された後に、
前記受付手段は、更に前記メンバー機器から、グループへの登録を解消することを示す脱退要求を受け付け、
前記通信手段は、更に、前記脱退要求が受け付けられると、前記共通秘密情報を削除することを指示する削除通知を前記メンバー機器へ出力し、
前記受付手段は、更に、前記共通秘密情報の削除が完了したことを示す完了通知を前記メンバー機器から受け付け、
前記判断手段は、更に、完了通知が受け付けられると、前記登録台数を減らす
ことを特徴とする請求項３のグループ管理機器。
【請求項１７】
前記判断手段は、前記登録台数が、前記制限台数より少ないと判断する場合、更に、前記メンバー機器において、前記共通秘密情報の使用を許可する期間を示す有効期限情報を発行し、
前記通信手段は、前記有効期限情報を前記メンバー機器へ出力し、
前記判断手段は、前記登録台数が、前記制限台数より少ないと判断する場合に、前記登録台数を増やし、更に、前記有効期限情報により示される期間の経過を監視しており、前記有効期限情報が示す期間が終了すると、前記登録台数を減らす
ことを特徴とする請求項３のグループ管理機器。
【請求項１８】
前記判断手段は、グループ外の管理装置から、グループに登録可能なクライアント機器の台数を取得し、取得した台数に応じて代金を支払い、取得した台数を前記制限台数とする
ことを特徴とする請求項３のグループ管理機器。
【請求項１９】
前記判断手段は、更に、グループ外の管理装置から新たに前記メンバー機器の登録可能な台数を取得し、取得した台数に応じて代金を支払い、前記制限台数に前記取得した台数を加算した台数を新たな制限台数とする
ことを特徴とする請求項３のグループ管理機器。
【請求項２０】
前記メンバー機器に対して前記共通秘密情報が出力された後に、
前記受付手段は、更に前記メンバー機器から、通信の要求を受け付け、
前記判断手段は、更に、前記共通秘密情報と要求元のメンバー機器が保持する共通秘密情報とを用いて認証し、
認証結果が成功の場合、前記通信手段は、更に、前記メンバー機器と通信を行う
ことを特徴とする請求項３のグループ管理機器。

【請求項２１】
前記グループ管理機器は、更に、
コンテンツ鍵を用いて暗号化した暗号化コンテンツと前記コンテンツ鍵とを蓄積しているコンテンツ格納手段と、
前記共通秘密情報を基に生成された鍵を用い、前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する暗号化手段とを備え、
前記通信手段は、更に、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵を前記メンバー機器へ出力する
ことを特徴とする請求項３のグループ管理機器。
【請求項２２】
前記判断手段は、更に、前記共通秘密情報と前記メンバー機器が保持する共通秘密情報とを用いて前記メンバー機器を認証し、前記共通秘密情報を用いて前記メンバー機器とセッション鍵を共有し、
前記暗号化手段は、前記認証が成功の場合に、前記共通秘密情報を基に生成された前記セッション鍵を用いて前記コンテンツ鍵を暗号化する
ことを特徴とする請求項２１のグループ管理機器。
【請求項２３】
前記通信手段は、前記共通秘密情報を記憶しており、更に、別の共通秘密情報を取得し、前記共通秘密情報に、前記別の共通秘密情報を上書きして記憶し、定期的又は不定期に取得した前記別の共通秘密情報を前記メンバー機器へ出力する
ことを特徴とする請求項３のグループ管理機器。
【請求項２４】
前記グループ管理機器は、更に、
コンテンツ鍵を用いて暗号化した暗号化コンテンツと前記コンテンツ鍵とを蓄積しているコンテンツ格納手段と、
前記共通秘密情報に基づいて生成される鍵を用いて、前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する暗号化手段と、
生成した暗号化コンテンツ鍵及び暗号化コンテンツを可搬型の記録媒体に書き込む書込手段とを備える
ことを特徴とする請求項３のグループ管理機器。
【請求項２５】
前記受付手段は、前記メンバー機器を識別する識別子を含む前記登録要求を受け付け、
前記暗号化手段は、前記登録要求に含まれる識別子と、前記共通秘密情報とから生成される鍵を用いて、前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する
ことを特徴とする請求項２４のグループ管理機器。
【請求項２６】
前記暗号化手段は、前記共通秘密情報及び前記記録媒体に固有の識別子に基づいて生成される鍵を用いて、前記コンテンツ鍵を暗号化する
ことを特徴とする請求項２４のグループ管理機器。
【請求項２７】
前記グループ管理機器は、更に、
複数のグループを識別する識別子に、前記グループのそれぞれに固有の共通秘密情報及び前記グループのそれぞれに登録可能な最大の台数である制限台数を対応付けて保持する保持手段を備え、
前記受付手段が、前記識別子の何れか一つを含む登録要求を受け付けると、前記判断手段は、前記受け付けた識別子が識別するグループに登録済みのメンバー機器の登録台数が、前記識別子に対応する前記制限台数より少ないか否かを判断し、少ないと判断される場合に、当該識別子が識別するグループにメンバー機器を登録し、前記識別子に対応する共通秘密情報を選択し、
前記通信手段は、選択された前記共通秘密情報を出力する

ことを特徴とする請求項３のグループ管理機器。
【請求項２８】
前記受付手段は、更に、前記新規のメンバー機器から、他の所定数のメンバー機器を登録する旨の登録要求を受け付け、
前記判断手段は、前記登録台数に前記所定数を加えた数が、前記制限台数を超えるか否かを判断し、超えないと判断する場合、前記所定数のメンバー機器への前記共通秘密情報の付与を許可する許可権利を生成し、
前記通信手段は、前記生成した許可権利を付加した前記共通秘密情報を前記新規のメンバー機器へ出力する
ことを特徴とする請求項３のグループ管理機器。
【請求項２９】
前記受付手段は、前記メンバー機器に固有の第１識別子を含む前記登録要求を受け付け、
前記判断手段は、更に、受け付けた前記第１識別子を記憶し、
前記通信手段が前記共通秘密情報を出力した後に、前記受付手段は、更に、メンバー機器に固有の第２識別子を受け付け、
前記判断手段は、更に、受け付けた第２識別子が、記憶している第１識別子と一致するか否かを判断し、
前記通信手段は、前記判断手段が一致すると判断する場合に、前記共通秘密情報を前記メンバー機器へ再度出力する
ことを特徴とする請求項３のグループ管理機器。
【請求項３０】
当該グループ管理機器が、複数のグループ管理機器が管理するグループを合わせて新たに形成する新グループを管理する新グループ管理機器になると決定された場合、前記通信手段は、新グループに固有の新共通秘密情報を、それぞれのメンバー機器へ出力し、
他のグループ管理機器が前記新グループ管理機器になると決定された場合、当該グループ管理機器は、更に、
前記他のグループ管理機器から、新グループに固有の新共通秘密情報を取得する取得手段と、
取得した前記新共通秘密情報を保持する保持手段とを備える
ことを特徴とする請求項３のグループ管理機器。
【請求項３１】
前記通信手段は、更に、他のグループを管理する他のグループ管理機器との間で、何れのグループ管理機器が、前記新グループ管理機器になるかを決定する
ことを特徴とする請求項３０のグループ管理機器。
【請求項３２】
前記保持手段は、更に、当該グループ管理機器に付された優先順位を記憶しており、
前記通信手段は、前記優先順位及び前記他のグループ管理機器に付された優先順位のうち、高い優先順位を付されたグループ管理機器を、前記新グループ管理機器になると決定する
ことを特徴とする請求項３１のグループ管理機器。
【請求項３３】
前記グループ管理機器及び他のグループ管理機器が管理するグループのメンバー機器は、それぞれ優先順位を付されており、
前記新グループ管理機器に決定された後、前記受付手段は、更に、各メンバー機器の優先順位を取得し、
前記グループ管理機器は、更に、
前記受付手段が取得した優先順位の高い機器から順に、前記制限台数以内で新グループに登録する新メンバー機器を選択する選択手段を備え、
前記通信手段は、選択した新メンバー機器へ前記新共通秘密情報を出力する
ことを特徴とする請求項３０のグループ管理機器。

【請求項３４】
前記グループ管理機器は、更に、
前記通信手段が前記共通秘密情報を出力した後、
当該グループ管理機器に登録されているメンバー機器から、別のグループを管理するグループ管理機器になるメンバー機器を選択する選択手段と、
当該グループに登録されている前記メンバー機器を、当該グループ管理機器が管理するグループのメンバー機器と、前記別のグループ管理機器が管理する別のグループのメンバー機器とに分ける分配手段とを備え、
前記通信手段は、当該グループ管理機器が管理するグループに分けられたメンバー機器に、前記共通秘密情報とは別の共通秘密情報を出力する
ことを特徴とする請求項３のグループ管理機器。
【請求項３５】
グループ管理機器に登録してコンテンツを利用するメンバー機器であって、
前記グループ管理機器にグループへの登録を要求する要求手段と、
前記グループ管理機器から認証を受け、グループに固有の共通秘密情報を取得する取得手段と、
取得した共通秘密情報を保持する保持手段と
から構成されることを特徴とするメンバー機器。
【請求項３６】
前記保持手段は、更に、第１初期値を保持し、
前記取得手段は、前記第１初期値を用いて前記グループ管理機器から認証を受け、認証結果が成功の場合に前記共通秘密情報を取得し、
前記保持手段は、取得した前記共通秘密情報を保持し、前記第１初期値の使用を抑制する
ことを特徴とする請求項３５のメンバー機器。
【請求項３７】
前記保持手段は、前記グループ管理機器に登録されていないことを示す前記第１初期値を保持する
ことを特徴とする請求項３６のメンバー機器。
【請求項３８】
前記保持手段は、当該メンバー機器が何れのグループ管理機器にも登録されていないことを示す前記第１初期値を保持する
ことを特徴とする請求項３６のメンバー機器。
【請求項３９】
前記保持手段は、保持している前記第１初期値に、取得した前記共通秘密情報を上書きする
ことを特徴とする請求項３６のメンバー機器。
【請求項４０】
前記共通秘密情報を取得し、前記保持手段により保持した後に、更に、
前記共通秘密情報を前記別のメンバー機器に出力する通信手段と、
前記通信手段が前記共通秘密情報を出力すると、前記保持手段により保持されている共通秘密情報を削除する削除手段とを備え、
前記保持手段は、前記共通秘密情報が削除されると、前記第１初期値を再度活性化する
ことを特徴とする請求項３６のメンバー機器。
【請求項４１】
前記要求手段は、更に、前記グループ管理機器に対してグループからの脱退を要求し、
前記取得手段は、更に、前記グループ管理機器から前記共通秘密情報を削除する旨の通知を取得し、
前記保持手段は、保持している前記共通秘密情報を削除し、前記第１初期値を再度活性化する

ことを特徴とする請求項３６のメンバー機器。
【請求項４２】
前記共通秘密情報を取得し、前記保持手段により保持した後に、
前記取得手段は、更に、前記グループ管理機器から前記共通秘密情報と異なる別の共通秘密情報を取得し、
前記保持手段は、前記共通秘密情報に、前記別の共通秘密情報を上書きする
ことを特徴とする請求項３５のメンバー機器。
【請求項４３】
前記要求手段は、更に、前記グループ管理機器へコンテンツの配送を要求し、
前記取得手段は、更に、前記グループ管理機器から、コンテンツ鍵を用いてコンテンツを暗号化して生成した暗号化コンテンツと、前記共通秘密情報を基に生成した暗号化鍵を用いて暗号化して生成した暗号化コンテンツ鍵とを取得し、
前記メンバー機器は、更に、
前記共通秘密情報を基に前記暗号化鍵と同一の復号鍵を生成し、生成した復号鍵を用いて前記暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、生成したコンテンツ鍵を用いて前記暗号化コンテンツを復号してコンテンツを生成する復号手段を備える
ことを特徴とする請求項３５のメンバー機器。
【請求項４４】
前記保持手段は、外部から読み出し及び書き込みを禁止された記憶部を備え、
前記記憶部は、前記グループ管理機器より取得する共通秘密情報を記憶し保持する
ことを特徴とする請求項３５のメンバー機器。
【請求項４５】
前記記憶部は、前記メンバー機器に着脱可能な記録媒体である
ことを特徴とする請求項４４のメンバー機器。
【請求項４６】
前記メンバー機器は、前記共通秘密情報を取得し、前記保持手段により保持した後に、更に、
前記別のメンバー機器と通信する際、前記共通秘密情報及び前記別のメンバー機器が保持する共通秘密情報を用いて前記別のメンバー機器を認証する認証手段を備える
ことを特徴とする請求項３５のメンバー機器。
【請求項４７】
前記メンバー機器は、前記共通秘密情報を取得し、前記保持手段により保持した後に、更に、
前記共通秘密情報を前記別のメンバー機器に出力する通信手段と、
前記通信手段が前記共通秘密情報を出力すると、前記保持手段により保持されている共通秘密情報を削除する削除手段とを備える
ことを特徴とする請求項３５のメンバー機器。
【請求項４８】
前記要求手段は、更に、前記グループ管理機器に対してグループからの脱退を要求し、
前記取得手段は、更に、前記グループ管理機器から前記共通秘密情報を削除する旨の通知を取得し、
前記保持手段は、保持している前記共通秘密情報を削除する
ことを特徴とする請求項３５のメンバー機器。
【請求項４９】
前記取得手段は、前記共通秘密情報の使用を許可される期間を示す有効期限情報を含む共通秘密情報を取得し、
前記保持手段は、前記有効期限情報が示す期間の経過を監視しており、前記期間が終了すると、前記共通秘密情報を削除する
ことを特徴とする請求項３５のメンバー機器。
【請求項５０】

前記要求手段、取得手段及び保持手段は、前記メンバー機器に着脱可能な可搬型モジュールであり、
前記可搬型モジュールは前記グループ管理機器に接続されると前記共通秘密情報を取得する
ことを特徴とする請求項３５のメンバー機器。
【請求項５１】
前記取得手段は、更に、コンテンツ鍵を用いて暗号化された暗号化コンテンツと、前記コンテンツ鍵を前記共通秘密情報を用いて生成された暗号化鍵を用いて暗号化して生成された暗号化コンテンツ鍵とを取得し、
前記メンバー機器は、更に、接続された前記可搬型モジュールから前記共通秘密情報を読み出し、読み出した共通秘密情報から前記暗号化鍵と同一の復号鍵を生成し、生成した復号鍵を用いて前記暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、前記コンテンツ鍵を用いて前記暗号化コンテンツを復号する復号手段を備える
ことを特徴とする請求項５０のメンバー機器。
【請求項５２】
前記可搬型モジュールは、更に、
前記保持手段が保持している前記共通秘密情報を前記メンバー機器へ通知する通知手段と、
前記共通秘密情報を前記メンバー機器へ通知した後に、前記通知手段に対して前記共通秘密情報をメンバー機器へ更に通知することを禁止する管理手段とを備え、
前記メンバー機器は、更に、
前記可搬型モジュールから前記共通秘密情報を取得して格納する格納手段を備える
ことを特徴とする請求項５０のメンバー機器。
【請求項５３】
前記保持手段は、更に、前記共通秘密情報を保持できる最大数を保持し、
前記要求手段は、前記保持手段が保持する共通秘密情報の数が、前記最大数に満たない場合、前記グループ管理機器に、グループへの登録を要求する
ことを特徴とする請求項３５のメンバー機器。
【請求項５４】
前記保持手段は、更に、複数のグループを識別する識別子を保持し、
前記要求手段は、前記識別子の何れか一つを付加して登録を要求し、
前記保持手段は、前記共通秘密情報を、前記登録要求に含めて送信した識別子と対応付けて記憶する
ことを特徴とする請求項５３のメンバー機器。
【請求項５５】
前記要求手段は、更に、所定数の他のメンバー機器の登録を要求し、
前記取得手段は、前記グループ管理機器から、更に、前記共通秘密情報を前記所定数のメンバー機器への付与を許可する許可権利を付加した前記共通秘密情報を取得し、
前記保持手段は、前記許可権利を付加した共通秘密情報を取得して保持し、
前記メンバー機器は、更に、
他のメンバー機器へ前記共通秘密情報を出力する通信手段を備え、
前記保持手段は、前記共通秘密情報が出力されると、前記許可権利から、前記共通秘密情報を前記他のメンバー機器へ付与する権利を１回分減らす
ことを特徴とする請求項３５のメンバー機器。
【請求項５６】
前記保持手段は、更に、当該メンバー機器に固有の識別子を保持し、
前記通信手段は、更に、前記他のメンバー機器から、当該他のメンバー機器に固有の識別子を取得し、
前記要求手段は、更に、前記グループ管理機器へ、当該メンバー機器と他のメンバー機器との識別子を送信する

ことを特徴とする請求項５５のメンバー機器。
【請求項５７】
前記メンバー機器は、更に、
前記保持手段は、更に、当該メンバー機器に固有の識別子を保持し、
前記要求手段は、更に、前記グループ管理機器へ前記識別子を送信し、
前記保持手段は、前記共通秘密情報を保持した後に、電源ＯＦＦの指示を受けると、保持した前記共通秘密情報を削除し、電源をＯＦＦにし、
電源がＯＮになると、前記要求手段は、前記識別子を前記グループ管理機器へ再度送信し、
前記グループ管理機器が、再度取得した識別子が前記記憶した識別子と一致する場合に、前記取得手段は、前記共通秘密情報を再取得する
ことを特徴とする請求項３５記載のメンバー機器。
【請求項５８】
前記メンバー機器は、更に、
前記保持手段は、更に、当該メンバー機器に固有の識別子を保持し、
前記要求手段は、更に、前記グループ管理機器へ前記識別子を送信し、
前記保持手段は、前記共通秘密情報を保持した後に、前記グループ管理機器との通信が遮断されると、保持した前記共通秘密情報を削除し、
前記グループ管理機器との通信が再度確立されると、前記要求手段は、前記識別子を前記グループ管理機器へ再度送信し、
前記グループ管理機器が再度取得した識別子が、前記記憶した識別子と一致する場合に、前記取得手段は、前記共通秘密情報を再取得する
ことを特徴とする請求項３５記載のメンバー機器。
【請求項５９】
前記共通秘密情報を保持した後、
前記取得手段は、前記グループ管理機器と同一又は別のグループ管理機器から、前記共通秘密情報とは別の共通秘密情報を取得し、
前記保持手段は、前記別の共通秘密情報を保持し、前記共通秘密情報の使用を抑制する
ことを特徴とする請求項３５のメンバー機器。
【請求項６０】
前記共通秘密情報を保持した後、前記グループ管理機器により、当該メンバー機器が前記グループ管理機器とは別の新グループ管理機器に選択されると、
更に、前記新グループ管理機器と前記グループ管理機器との間で、前記グループ管理機器に登録されていた元のメンバー機器を、前記グループ管理機器に登録するメンバー機器と、前記新グループ管理機器に登録するメンバー機器とに分ける選択手段と、
前記新グループ管理機器が管理する新グループに固有の新共通秘密情報を、当該新グループ管理機器に選択された前記メンバー機器へ出力する通信手段とを備える
ことを特徴とする請求項３５のメンバー機器。
【請求項６１】
前記グループ管理機器に登録されているメンバー機器はそれぞれ優先順位を付されており、
前記取得手段は、他のメンバー機器の前記優先順位を取得し、
前記選択手段は、取得した優先順位を基に、メンバー機器を分ける
ことを特徴とする請求項６０のメンバー機器。
【請求項６２】
メンバー機器をグループ管理機器に登録する登録機器であって、
前記グループ管理機器からグループに固有の共通秘密情報を取得し、保持する保持手段と、
前記メンバー機器に接続されると、当該メンバー機器に前記共通秘密情報を通知する通知手段と

から構成されることを特徴とする登録機器。
【請求項６３】
前記登録機器は、更に、
前記共通秘密情報を前記メンバー機器へ通知した後に、前記通知手段に対して前記共通秘密情報をメンバー機器へ更に通知することを禁止する管理手段を備える
ことを特徴とする請求項６２記載の登録装置。
【請求項６４】
前記登録機器は、更に、
前記メンバー機器から、前記共通秘密情報の取得の要求を受け付ける受付手段を備え、
前記通知手段は、前記要求を受け付けた場合に、前記共通秘密情報を通知する
ことを特徴とする請求項６２記載の登録装置。
【請求項６５】
グループ管理機器に登録してコンテンツを利用するメンバー機器であって、
前記グループ管理機器との距離、前記グループ管理機器との通信時間、前記グループ管理機器の処理能力又は前記グループ管理機器の処理状態のうち、予め設定された条件を基にして、複数のグループ管理機器から、１個のグループ管理機器を選択する選択手段と、
選択したグループ管理機器に登録を要求する要求手段と、
前記グループ管理機器から、グループ内で共通の共通秘密情報を取得する取得手段と、
取得した共通秘密情報を保持する保持手段と
から構成されることを特徴とするメンバー機器。
【請求項６６】
グループを管理するグループ管理機器で用いられる認証方法であって、
メンバー機器から要求を受け付ける受付ステップと、
当該グループ管理機器により管理されるグループに固有の共通秘密情報と、前記要求元のメンバー機器が保持する共通秘密情報とを用いて前記メンバー機器が正当な機器であるか否かを認証する認証ステップと、
認証結果が成功の場合、前記メンバー機器は前記グループに登録されていると判断する判断ステップと
を含むことを特徴とする方法。
【請求項６７】
グループを管理するグループ管理機器で用いられるプログラムであって、
メンバー機器から要求を受け付ける受付ステップと、
当該グループ管理機器により管理されるグループに固有の共通秘密情報と、前記要求元のメンバー機器が保持する共通秘密情報とを用いて前記メンバー機器が正当な機器であるか否かを認証する認証ステップと、
認証結果が成功の場合、前記メンバー機器は前記グループに登録されていると判断する判断ステップと
を含むことを特徴とするプログラム。
【請求項６８】
グループを管理するグループ管理機器で用いられるプログラムを記録した記録媒体であって、前記プログラムは、
メンバー機器から要求を受け付ける受付ステップと、
当該グループ管理機器により管理されるグループに固有の共通秘密情報と、前記要求元のメンバー機器が保持する共通秘密情報とを用いて前記メンバー機器が正当な機器であるか否かを認証する認証ステップと、
認証結果が成功の場合、前記メンバー機器は前記グループに登録されていると判断する判断ステップと
を含むことを特徴とする記録媒体。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、ディジタルコンテンツの利用が相互に可能なグループを形成し、管理するグループ形成管理システムに関する。
【背景技術】
【０００２】
近年、音楽や映像、ゲームなどのディジタル著作物（以下、コンテンツ）は、インターネットやデジタル放送、パッケージメディアによる流通により容易に取得が可能となってきている。
特許文献１によると、正当な権利を有さない第三者の利用を防止しつつ、所望の情報処置装置でコンテンツを利用できるようにすることを目的として、音楽データ管理システムが開示されている。
【０００３】
前記音楽データ管理システムにおいて、複数のパーソナルコンピュータ（以下、PC）は、PCのコンテンツ管理プログラムのIDと共に、クレジットカードの番号などを承認サーバに送信する。
承認サーバは、ID、クレジットカードの番号などを受信する。クレジットカードの番号が同じであれば、PCを同じグループに分類する。各グループについて、ID、クレジットカードの番号などを記録することにより、PC及び使用者を登録する。登録が終了したとき、承認サーバは、グループのIDおよびパスワードと共に、グループ鍵をPCに送信する。
【０００４】
PCは受信したグループ鍵、グループのIDおよびパスワードを記憶する。
こうして、同一のグループ鍵を有するPCは、グループ鍵を用いてコンテンツの送受信を行うことが出来る。
この技術では、如何なる機器でもグループ内の機器として登録可能であり、１個のグループに登録される機器を自由に増やすことが出来る。
【０００５】
また、非特許文献１によると、DTCP（Digital Transmission Content Protection）と呼ばれる規格が開示されている。
DTCPは、高速シリアルバス規格の一つであるIEEE1394により規定されるバスを介して配信されるディジタルコンテンツの保護規格である。コンテンツを利用する機器はそれぞれ、DTLA（Digital Transmission Licensing Administrator）と呼ばれる管理者との契約に基づいて配布された秘密鍵を備えている。コンテンツを視聴する際、送信機器と受信機器とは秘密鍵を用いて相互認証を行い、認証に成功した受信機器がコンテンツを視聴できる。
【０００６】
この技術では、DTLAから秘密鍵を配布された機器であれば、コンテンツ利用の都度、異なる機器がグループを形成してコンテンツを利用する。
【特許文献１】特開２００２－１６９７２６号公報
【非特許文献１】「５C Digital Transmission Content Protection White Paper」Revision１．０ July 14,1998
【発明の開示】
【発明が解決しようとする課題】
【０００７】
このように、特許文献１及び非特許文献１により開示された技術によると、グループを形成し、グループ内に含まれる機器間でのコンテンツの利用を許可されるものの、著作権保護の観点からは、グループを形成する機器をより固定的にしたいという要望があり、一方ユーザ側からは、IEEE1394バスといった物理的に伝送範囲が制限された範囲だけでなく、例えばIP（Internet Protocol）を用いて、より広い範囲で自由にコンテンツを利用したいという要望がある。
【０００８】

そこで本発明は、グループの範囲をより固定的にし、グループ内の機器間ではコンテンツを自由に利用可能なグループ形成管理システム、グループ管理機器及びメンバー機器を提供することを目的とする。

【課題を解決するための手段】

【０００９】

上記目的を達成するために本発明は、グループに固有の共通秘密情報を保持している１個以上の登録済のメンバー機器と、　グループへの登録の要求を送信し、共通秘密情報を取得して保持する新規のメンバー機器と、新規のメンバー機器から登録の要求を受け付け、グループに登録されている前記登録済のメンバー機器の台数が、グループに登録可能な最大の台数である制限台数未満の場合、前記新規のメンバー機器を登録し、当該メンバー機器へ前記共通秘密情報を出力するグループ管理機器とから構成されることを特徴とするグループ形成管理システムである。

【００１０】

また、グループへのメンバー機器の登録を管理するグループ管理機器であって、前記メンバー機器からグループに登録する旨の登録要求を受け付ける受付手段と、登録要求が受け付けられると、前記メンバー機器が正当な機器であれば、グループに登録済みのメンバー機器の登録台数が、グループに登録可能な最大の台数である制限台数より少ないか否かを判断し、少ないと判断する場合、前記メンバー機器を登録する判断手段と、前記制限台数より少ないと判断する場合に、前記メンバー機器へグループに固有の共通秘密情報を出力する通信手段とから構成されることを特徴とするグループ管理機器である。

【００１１】

また、グループ管理機器に登録してコンテンツを利用するメンバー機器であって、前記グループ管理機器にグループへの登録を要求する要求手段と、前記グループ管理機器から認証を受け、グループに固有の共通秘密情報を取得する取得手段と、取得した共通秘密情報を保持する保持手段とから構成されることを特徴とするメンバー機器である。

これによって、登録済みのメンバー機器が制限台数未満であれば、新規のメンバー機器に共通秘密情報を出力するので、グループに登録するメンバー機器の台数を制限し、グループの範囲をより固定的にすることが出来る。

【００１２】

また、本発明はメンバー機器をグループ管理機器に登録する登録機器であって、前記グループ管理機器からグループに固有の共通秘密情報を取得し、保持する保持手段と、前記メンバー機器に接続されると、当該メンバー機器に前記共通秘密情報を通知する通知手段とから構成されることを特徴とする登録機器である。

これにより、グループ管理機器と直接通信する機能を備えていないメンバー機器もグループに登録することが出来る。

【発明の効果】

【００１３】

本発明は、グループに固有の共通秘密情報を保持している１個以上の登録済のメンバー機器と、グループへの登録の要求を送信し、共通秘密情報を取得して保持する新規のメンバー機器と、新規のメンバー機器から登録の要求を受け付け、グループに登録されている前記登録済のメンバー機器の台数が、グループに登録可能な最大の台数である制限台数未満の場合、前記新規のメンバー機器を登録し、当該メンバー機器へ前記共通秘密情報を出力するグループ管理機器とから構成されることを特徴とするグループ形成管理システムである。

【００１４】

また、グループ形成管理システムであって、グループへの登録の要求を送信し、グループに固有の共通秘密情報を取得して保持するメンバー機器と、前記メンバー機器から登録の要求を受け付け、グループに登録されているメンバー機器の台数が、グループに登録可能な最大の台数である制限台数未満の場合、前記メンバー機器を登録し、当該メンバー機器へ前記共通秘密情報を出力するグループ管理機器とから構成され、初期の状態では、前

記グループ管理機器にメンバー機器は登録されていないことを特徴とするグループ形成管理システムである。

【００１５】

また、グループへのメンバー機器の登録を管理するグループ管理機器であって、前記メンバー機器からグループに登録する旨の登録要求を受け付ける受付手段と、登録要求が受け付けられると、前記メンバー機器が正当な機器であれば、グループに登録済みのメンバー機器の登録台数が、グループに登録可能な最大の台数である制限台数より少ないか否かを判断し、少ないと判断する場合、前記メンバー機器を登録する判断手段と、前記制限台数より少ないと判断する場合に、前記メンバー機器へグループに固有の共通秘密情報を出力する通信手段とから構成されることを特徴とするグループ管理機器である。

【００１６】

また、グループ管理機器に登録してコンテンツを利用するメンバー機器であって、前記グループ管理機器にグループへの登録を要求する要求手段と、前記グループ管理機器から認証を受け、グループに固有の共通秘密情報を取得する取得手段と、取得した共通秘密情報を保持する保持手段とから構成されることを特徴とするメンバー機器である。

この構成によると、登録済みのメンバー機器が制限台数未満であれば、新規のメンバー機器に共通秘密情報を出力するので、グループに登録するメンバー機器の台数を制限し、グループの範囲をより固定的にすることが出来る。

できる。

【００１７】

ここで、前記メンバー機器は、第1初期値を保持し、前記判断手段は、第2初期値を保持し、前記第2初期値と前記第1初期値とを用いて前記メンバー機器の正当性を認証する認証手段と、前記認証結果が成功の場合、前記登録台数が前記制限台数より少ないか否かを判断する台数判断手段とを含み、前記通信手段は、前記共通秘密情報として、当該グループ管理機器により管理されるグループに登録されたことを示す共通秘密情報を出力し、前記メンバー機器は、前記共通秘密情報を取得して保持し、前記第１初期値の使用を抑制するとしても良い。

【００１８】

また、前記メンバー機器は、前記グループ管理機器に登録されていないことを示す前記第１初期値を保持し、前記認証手段は、当該グループ管理機器に登録されていないことを示す前記第２初期値と、前記第１初期値とを用いて認証するとしても良い。

また、前記メンバー機器は、当該メンバー機器が何れのグループ管理機器にも登録されていないことを示す前記第１初期値を保持し、前記認証手段は、前記メンバー機器が何れのグループ管理機器にも登録されていないことを示す前記第２初期値と、前記第１初期値とを用いて認証するとしても良い。

【００１９】

また、前記保持手段は、更に、第１初期値を保持し、前記取得手段は、前記第１初期値を用いて前記グループ管理機器から認証を受け、認証結果が成功の場合に前記共通秘密情報を取得し、前記保持手段は、取得した前記共通秘密情報を保持し、前記第１初期値の使用を抑制するとしても良い。

また、前記保持手段は、前記グループ管理機器に登録されていないことを示す前記第１初期値を保持するとしても良い。

【００２０】

また、前記保持手段は、当該メンバー機器が何れのグループ管理機器にも登録されていないことを示す前記第１初期値を保持するとしても良い。

また、前記保持手段は、保持している前記第１初期値に、取得した前記共通秘密情報を上書きするとしても良い。

この構成によると、メンバー機器が保持する第１初期値と、グループ管理機器が保持する第２初期値とを用いて認証するため、メンバー機器が初期値を保持している場合、グループに未登録であると判断することが出来る。

【００２１】
ここで、前記共通秘密情報を取得し、前記保持手段により保持した後に、更に、前記共通秘密情報を前記別のメンバー機器に出力する通信手段と、前記通信手段が前記共通秘密情報を出力すると、前記保持手段により保持されている共通秘密情報を削除する削除手段とを備え、前記保持手段は、前記共通秘密情報が削除されると、前記第１初期値を再度活性化するとしても良い。
【００２２】
また、前記要求手段は、更に、前記グループ管理機器に対してグループからの脱退を要求し、前記取得手段は、更に、前記グループ管理機器から前記共通秘密情報を削除する旨の通知を取得し、前記保持手段は、保持している前記共通秘密情報を削除し、前記第１初期値を再度活性化するとしても良い。
この構成によると、共通秘密情報を削除したメンバー機器は、第１初期値を再度活性化するため、初期値を保持しているメンバー機器として、グループに登録できる。
【００２３】
ここで、前記グループ管理機器は、更に、前記共通秘密情報を生成する生成手段を備え、前記通信手段は、生成された前記共通秘密情報を出力するとしても良い。
この構成によると、グループ管理機器が共通秘密情報を生成するので、グループ内の機器のみでグループを管理することが出来る。
ここで、グループ外の管理装置により前記共通秘密情報を生成され、前記判断手段は、グループ外の前記管理装置から前記共通秘密情報を取得し、前記通信手段は、取得した前記共通秘密情報を前記メンバー機器へ出力するとしても良い。
【００２４】
この構成によると、グループ外の管理装置により、共通秘密情報が生成されるので、他のグループの共通秘密情報と重複しない共通秘密情報を生成することが出来る。
ここで、前記受付手段は、前記登録要求を受け付けると、グループ外の管理装置に前記登録要求を受け付けた旨を通知し、前記グループ外の管理装置は、前記登録台数が、前記グループに登録可能な最大の台数である制限台数より少ないか否かを判断し、前記判断手段は、前記登録台数が前記制限台数より少ないか否かを判断する代わりに、前記管理装置から判断結果を受け取り、前記通信手段は、前記判断結果が、前記台数より前記制限台数の方が少ないことを示す場合、前記共通秘密情報を出力するとしても良い。
【００２５】
この構成によると、登録台数が制限台数より少ないか否かをグループ外の管理装置が判断するので、グループ管理機器での処理を減らすことが出来る。
ここで、前記制限台数は、第1制限台数と第2制限台数とから成り、前記判断手段は、登録済みのメンバー機器の台数が、前記第1制限台数又は前記第２制限台数より少ないか否かを判断するとしても良い。
【００２６】
ここで、前記第1制限台数は、前記制限台数のうち、当該グループ管理機器に接続可能なメンバー機器の最大の台数であり、前記第２制限台数は、前記制限台数のうち、当該グループ管理機器に接続できないメンバー機器の最大の台数であり、前記判断手段は、前記要求元のメンバー機器が当該グループ管理機器に接続可能なメンバー機器である場合、登録済みの接続可能なメンバー機器の台数が、前記第1制限台数より少ないか否かを判断し、前記要求元のメンバー機器が当該グループ管理機器に接続できないメンバー機器である場合、登録済みの接続できないメンバー機器の台数が、前記第２制限台数より少ないか否かを判断するとしても良い。
【００２７】
この構成によると、第１制限台数と第２制限台数とを基に、メンバー機器をグループに登録する台数を制限しているので、ユーザの要望に沿った台数管理ができる。
ここで、前記通信手段は、更に、他のグループ管理機器に、前記メンバー機器を登録可能であるか否かを問い合わせる問合要求を出力し、前記他のグループ管理機器は、前記問

合要求を受け付け、前記他のグループ管理機器に登録済みのメンバー機器の登録台数が、当該他のグループ管理機器の制限台数より少ないか否かを判断し、少ないと判断する場合、前記メンバー機器を登録し、前記グループ管理機器へ前記共通秘密情報を出力し、前記通信手段は、前記他のグループ管理機器から前記共通秘密情報を受信すると、前記メンバー機器へ前記共通秘密情報を出力するとしても良い。

【００２８】

この構成によると、一つのグループ内に複数のグループ管理機器が有る場合に、メンバー機器は、登録を要求したグループ管理機器に登録できなくても、そのグループ管理機器が登録可能な他の機器を探すため、グループに登録することが出来る。

ここで、前記判断手段は、外部からの不正なアクセスに対抗する機能を備え、前記制限台数及び前記共通秘密情報は、外部から読み出し及び書き込みが出来ない領域内に記憶されているとしても良い。

【００２９】

また、前記保持手段は、外部から読み出し及び書き込みを禁止された記憶部を備え、前記記憶部は、前記グループ管理機器より取得する共通秘密情報を記憶し保持するとしても良い。

また、前記記憶部は、前記メンバー機器に着脱可能な記録媒体であるとしても良い。

この構成によると、グループ管理機器において、制限台数及び共通秘密情報は、読み出し書き込み不可能な記憶部に記憶され、メンバー機器においても共通秘密情報は、同様の記憶部に記憶されるので、外部に知られたり、書き換えられたりすることなく保持される。

【００３０】

また、前記判断手段は、前記グループ管理機器に着脱可能な可搬型モジュールから構成されているとしても良い。

この構成によると、グループ管理機器では、メンバー機器を登録可能か否かの判断をICカードが行うため、任意の機器にICカードを装着し、AD内サーバとすることが出来る。

ここで、前記判断手段は、前記制限台数から前記登録台数を差し引いた残数を記憶し、前記受付手段が登録要求を受け付けると、前記残数が「０」であるか否かを判断し、「０」でないと判断する場合、前記通信手段は、前記メンバー機器へ前記共通秘密情報を出力し、「０」でないと判断する場合、前記判断手段は、前記残数から「１」を減算するとしても良い。

【００３１】

この構成によると、残数が「０」でない場合に、メンバー機器を登録するので、グループに登録されている機器の台数を制限することが出来る。

ここで、前記メンバー機器に対して前記共通秘密情報が出力された後に、前記受付手段は、更に前記メンバー機器から、グループへの登録を解消することを示す脱退要求を受け付け、前記通信手段は、更に、前記脱退要求が受け付けられると、前記共通秘密情報を削除することを指示する削除通知を前記メンバー機器へ出力し、前記受付手段は、更に、前記共通秘密情報の削除が完了したことを示す完了通知を前記メンバー機器から受け付け、前記判断手段は、更に、完了通知が受け付けられると、前記登録台数を減らすとしても良い。

【００３２】

また、前記要求手段は、更に、前記グループ管理機器に対してグループからの脱退を要求し、前記取得手段は、更に、前記グループ管理機器から前記共通秘密情報を削除する旨の通知を取得し、前記保持手段は、保持している前記共通秘密情報を削除するとしても良い。

この構成によると、グループ管理機器は、登録済みのメンバー機器がグループから脱退する際、登録台数を減らすので、グループに登録できる機器を一定の台数に保つことが出来る。また、メンバー機器は、共通秘密情報を削除するので、グループから脱退したメンバー機器によるコンテンツの利用を防止することが出来る。

【００３３】
ここで、前記判断手段は、前記登録台数が、前記制限台数より少ないと判断する場合、更に、前記メンバー機器において、前記共通秘密情報の使用を許可する期間を示す有効期限情報を発行し、前記通信手段は、前記有効期限情報を前記メンバー機器へ出力し、前記判断手段は、前記登録台数が、前記制限台数より少ないと判断する場合に、前記登録台数を増やし、更に、前記有効期限情報により示される期間の経過を監視しており、前記有効期限情報が示す期間が終了すると、前記登録台数を減らすとしても良い。
【００３４】
また、前記取得手段は、前記共通秘密情報の使用を許可される期間を示す有効期限情報を含む共通秘密情報を取得し、前記保持手段は、前記有効期限情報が示す期間の経過を監視しており、前記期間が終了すると、前記共通秘密情報を削除するとしても良い。
この構成によると、有効期限情報が示す期間だけ、メンバー機器にコンテンツの利用を許可するので、メンバー機器が、グループ管理機器とオンラインで接続されていなくても、一旦登録の処理を行うとそれぞれの機器で共通秘密情報を管理することが出来る。また、メンバー機器では共通秘密情報を削除し、グループ管理機器では登録台数を減らすので、グループに登録可能な台数は一定に保つことが出来る。
【００３５】
ここで、前記判断手段は、グループ外の管理装置から、グループに登録可能なクライアント機器の台数を取得し、取得した台数に応じて代金を支払い、取得した台数を前記制限台数とするとしても良い。
この構成によると、グループ管理機器は、制限台数を設定する際に代金を支払うので、管理装置は、台数に応じて課金することが出来る。また、制限台数
を柔軟に設定することが出来る。
【００３６】
ここで、前記判断手段は、更に、グループ外の管理装置から新たに前記メンバー機器の登録可能な台数を取得し、取得した台数に応じて代金を支払い、前記制限台数に前記取得した台数を加算した台数を新たな制限台数とするとしても良い。
この構成によると、制限台数を増やすことが出来、台数に応じて課金することが出来るため、グループに登録可能な機器の台数を柔軟に管理することが出来る。
【００３７】
ここで、前記メンバー機器に対して前記共通秘密情報が出力された後に、前記受付手段は、更に前記メンバー機器から、通信の要求を受け付け、前記判断手段は、更に、前記共通秘密情報と要求元のメンバー機器が保持する共通秘密情報とを用いて認証し、認証結果が成功の場合、前記通信手段は、更に、前記メンバー機器と通信を行うとしても良い。
また、前記メンバー機器は、前記共通秘密情報を取得し、前記保持手段により保持した後に、更に、前記別のメンバー機器と通信する際、前記共通秘密情報及び前記別のメンバー機器が保持する共通秘密情報を用いて前記別のメンバー機器を認証する認証手段を備えるとしても良い。
【００３８】
この構成によると、認証相手の機器が保持する共通秘密情報の値と自身が保持する共通秘密情報とを用いて認証するため、相手機器が同一のグループに登録されているか否かを確認することが出来る。
ここで、前記グループ管理機器は、更に、コンテンツ鍵を用いて暗号化した暗号化コンテンツと前記コンテンツ鍵とを蓄積しているコンテンツ格納手段と、前記共通秘密情報を基に生成された鍵を用い、前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する暗号化手段とを備え、前記通信手段は、更に、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵を前記メンバー機器へ出力するとしても良い。
【００３９】
また、前記要求手段は、更に、前記グループ管理機器へコンテンツの配送を要求し、前記取得手段は、更に、前記グループ管理機器から、コンテンツ鍵を用いてコンテンツを暗

号化して生成した暗号化コンテンツと、前記共通秘密情報を基に生成した暗号化鍵を用いて暗号化して生成した暗号化コンテンツ鍵とを取得し、前記メンバー機器は、更に、前記共通秘密情報を基に前記暗号化鍵と同一の復号鍵を生成し、生成した復号鍵を用いて前記暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、生成したコンテンツ鍵を用いて前記暗号化コンテンツを復号してコンテンツを生成する復号手段を備えるとしても良い。

【００４０】

この構成によると、共通秘密情報を基にした鍵を用いてコンテンツ鍵を暗号化するため、コンテンツを利用可能な機器を、共通秘密情報を保持する機器に限定することが出来る。

また、前記判断手段は、更に、前記共通秘密情報と前記メンバー機器が保持する共通秘密情報とを用いて前記メンバー機器を認証し、前記共通秘密情報を用いて前記メンバー機器とセッション鍵を共有し、前記暗号化手段は、前記認証が成功の場合に、前記共通秘密情報を基に生成された前記セッション鍵を用いて前記コンテンツ鍵を暗号化するとしても良い。

【００４１】

この構成によると、共通秘密情報を用いてメンバー機器を認証するため、同一のグループに登録されていることを確認できた機器のみに、コンテンツの利用を許可することが出来る。また、共通秘密情報に依存したセッション鍵を用いてコンテンツ鍵を暗号化しているので、共通秘密情報を保持しない機器ではコンテンツを利用できない。

ここで、前記通信手段は、前記共通秘密情報を記憶しており、更に、別の共通秘密情報を取得し、前記共通秘密情報に、前記別の共通秘密情報を上書きして記憶し、定期的又は不定期に取得した前記別の共通秘密情報を前記メンバー機器へ出力するとしても良い。

【００４２】

また、前記共通秘密情報を取得し、前記保持手段により保持した後に、前記取得手段は、更に、前記グループ管理機器から前記共通秘密情報と異なる別の共通秘密情報を取得し、前記保持手段は、前記共通秘密情報に、前記別の共通秘密情報を上書きするとしても良い。

この構成によると、グループの共通秘密情報を定期的又は不定期に更新するため、仮に共通秘密情報が外部の機器に知られたとしても、共通秘密情報を更新するので、更新されていない機器でのコンテンツの利用を防止することが出来る。

【００４３】

ここで、前記グループ管理機器は、更に、コンテンツ鍵を用いて暗号化した暗号化コンテンツと前記コンテンツ鍵とを蓄積しているコンテンツ格納手段と、前記共通秘密情報に基づいて生成される鍵を用いて、前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する暗号化手段と、生成した暗号化コンテンツ鍵及び暗号化コンテンツを可搬型の記録媒体に書き込む書込手段とを備えるとしても良い。

【００４４】

また、前記受付手段は、前記メンバー機器を識別する識別子を含む前記登録要求を受け付け、前記暗号化手段は、前記登録要求に含まれる識別子と、前記共通秘密情報とから生成される鍵を用いて、前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成するとしても良い。

また、前記暗号化手段は、前記共通秘密情報及び前記記録媒体に固有の識別子に基づいて生成される鍵を用いて、前記コンテンツ鍵を暗号化するとしても良い。

【００４５】

この構成によると、共通秘密情報に基づいて生成される鍵を用いてコンテンツ鍵を暗号化して記録するため、共通秘密情報を保持しない機器でのコンテンツの利用を防止することが出来る。また、共通秘密情報と、グループに登録している機器の識別子とを用いて生成される鍵を用いてコンテンツ鍵を暗号化するため、登録している識別子の機器でのみ使用可能になり、他の不正な機器によるコンテンツの利用を防止することが出来る。

【００４６】

ここで、前記グループ管理機器は、更に、複数のグループを識別する識別子に、前記グループのそれぞれに固有の共通秘密情報及び前記グループのそれぞれに登録可能な最大の台数である制限台数を対応付けて保持する保持手段を備え、前記受付手段が、前記識別子の何れか一つを含む登録要求を受け付けると、前記判断手段は、前記受け付けた識別子が識別するグループに登録済みのメンバー機器の登録台数が、前記識別子に対応する前記制限台数より少ないか否かを判断し、少ないと判断される場合に、当該識別子が識別するグループにメンバー機器を登録し、前記識別子に対応する共通秘密情報を選択し、前記通信手段は、選択された前記共通秘密情報を出力するとしても良い。

【００４７】

この構成によると、１台のグループ管理機器で複数のグループを管理することが出来る。

ここで、前記受付手段は、更に、前記新規のメンバー機器から、他の所定数のメンバー機器を登録する旨の登録要求を受け付け、前記判断手段は、前記登録台数に前記所定数を加えた数が、前記制限台数を超えるか否かを判断し、超えないと判断する場合、前記所定数のメンバー機器への前記共通秘密情報の付与を許可する許可権利を生成し、前記通信手段は、前記生成した許可権利を付加した前記共通秘密情報を前記新規のメンバー機器へ出力するとしても良い。

【００４８】

また、前記要求手段は、更に、所定数の他のメンバー機器の登録を要求し、前記取得手段は、前記グループ管理機器から、更に、前記共通秘密情報を前記所定数のメンバー機器への付与を許可する許可権利を付加した前記共通秘密情報を取得し、前記保持手段は、前記許可権利を付加した共通秘密情報を取得して保持し、前記メンバー機器は、更に、他のメンバー機器へ前記共通秘密情報を出力する通信手段を備え、前記保持手段は、前記共通秘密情報が出力されると、前記許可権利から、前記共通秘密情報を前記他のメンバー機器へ付与する権利を１回分減らすとしても良い。

【００４９】

また、前記保持手段は、更に、当該メンバー機器に固有の識別子を保持し、前記通信手段は、更に、前記他のメンバー機器から、当該他のメンバー機器に固有の識別子を取得し、前記要求手段は、更に、前記グループ管理機器へ、当該メンバー機器と他のメンバー機器との識別子を送信するとしても良い。

この構成によると、新規のメンバー機器は、複数のメンバー機器の代表として、グループ管理機器から共通秘密情報を取得し、他の所定数のメンバー機器に共通秘密情報を付与するため、複数のメンバー機器を一度に登録することが出来る。また、所定数のメンバー機器がグループ管理機器と直接通信する機能を備えなくても、代表のメンバー機器が通信機能を備えていれば、他の所定数のメンバー機器を登録することが出来る。また、メンバー機器それぞれのIDを登録するため、コンテンツ配送の際などに、IDを登録している機器に限定することが出来る。

【００５０】

ここで、前記受付手段は、前記メンバー機器に固有の第１識別子を含む前記登録要求を受け付け、前記判断手段は、更に、受け付けた前記第１識別子を記憶し、前記通信手段が前記共通秘密情報を出力した後に、前記受付手段は、更に、メンバー機器に固有の第２識別子を受け付け、前記判断手段は、更に、受け付けた第２識別子が、記憶している第１識別子と一致するか否かを判断し、前記通信手段は、前記判断手段が一致すると判断する場合に、前記共通秘密情報を前記メンバー機器へ再度出力するとしても良い。

【００５１】

また、前記メンバー機器は、更に、前記保持手段は、更に、当該メンバー機器に固有の識別子を保持し、前記要求手段は、更に、前記グループ管理機器へ前記識別子を送信し、前記保持手段は、前記共通秘密情報を保持した後に、電源ＯＦＦの指示を受けると、保持した前記共通秘密情報を削除し、電源をＯＦＦにし、電源がＯＮになると、前記要求手段は、前記識別子を前記グループ管理機器へ再度送信し、前記グループ管理機器が、再度取

得した識別子が前記記憶した識別子と一致する場合に、前記取得手段は、前記共通秘密情報を再取得するとしても良い。

【００５２】

また、前記メンバー機器は、更に、前記保持手段は、更に、当該メンバー機器に固有の識別子を保持し、前記要求手段は、更に、前記グループ管理機器へ前記識別子を送信し、前記保持手段は、前記共通秘密情報を保持した後に、前記グループ管理機器との通信が遮断されると、保持した前記共通秘密情報を削除し、前記グループ管理機器との通信が再度確立されると、前記要求手段は、前記識別子を前記グループ管理機器へ再度送信し、前記グループ管理機器が再度取得した識別子が、前記記憶した識別子と一致する場合に、前記取得手段は、前記共通秘密情報を再取得するとしても良い。

【００５３】

この構成によると、メンバー機器は、通信が遮断された場合、又は電源をOFFにした場合に共通秘密情報を削除し、必要に応じて共通秘密情報を取得するため、不正に共通秘密情報を利用されることを防ぐ。

ここで、当該グループ管理機器が、複数のグループ管理機器が管理するグループを合わせて新たに形成する新グループを管理する新グループ管理機器になると決定された場合、前記通信手段は、新グループに固有の新共通秘密情報を、それぞれのメンバー機器へ出力し、他のグループ管理機器が前記新グループ管理機器になると決定された場合、当該グループ管理機器は、更に、前記他のグループ管理機器から、新グループに固有の新共通秘密情報を取得する取得手段と、取得した前記新共通秘密情報を保持する保持手段とを備えるとしても良い。

【００５４】

また、前記通信手段は、更に、他のグループを管理する他のグループ管理機器との間で、何れのグループ管理機器が、前記新グループ管理機器になるかを決定するとしても良い。

また、前記保持手段は、更に、当該グループ管理機器に付された優先順位を記憶しており、前記通信手段は、前記優先順位及び前記他のグループ管理機器に付された優先順位のうち、高い優先順位を付されたグループ管理機器を、前記新グループ管理機器になると決定するとしても良い。

【００５５】

また、前記共通秘密情報を保持した後、前記取得手段は、前記グループ管理機器と同一又は別のグループ管理機器から、前記共通秘密情報とは別の共通秘密情報を取得し、前記保持手段は、前記別の共通秘密情報を保持し、前記共通秘密情報の使用を抑制するとしても良い。

この構成によると、複数のグループを合わせて一つのグループを形成することが出来る。

【００５６】

ここで、前記グループ管理機器及び他のグループ管理機器が管理するグループのメンバー機器は、それぞれ優先順位を付されており、前記新グループ管理機器に決定された後、前記受付手段は、更に、各メンバー機器の優先順位を取得し、　前記グループ管理機器は、更に、前記受付手段が取得した優先順位の高い機器から順に、前記制限台数以内で新グループに登録する新メンバー機器を選択する選択手段を備え、前記通信手段は、選択した新メンバー機器へ前記新共通秘密情報を出力するとしても良い。

【００５７】

この構成によると、複数のグループを組み合わせた際に、メンバー機器が制限台数を超えても、優先順位によって登録するメンバー機器を選択し、制限台数以内に制限することが出来る。

ここで、前記グループ管理機器は、更に、前記通信手段が前記共通秘密情報を出力した後、当該グループ管理機器に登録されているメンバー機器から、別のグループを管理するグループ管理機器になるメンバー機器を選択する選択手段と、当該グループに登録されて

いる前記メンバー機器を、当該グループ管理機器が管理するグループのメンバー機器と、前記別のグループ管理機器が管理する別のグループのメンバー機器とに分ける分配手段とを備え、前記通信手段は、当該グループ管理機器が管理するグループに分けられたメンバー機器に、前記共通秘密情報とは別の共通秘密情報を出力するとしても良い。

【００５８】

また、前記共通秘密情報を保持した後、前記グループ管理機器により、当該メンバー機器が前記グループ管理機器とは別の新グループ管理機器に選択されると、更に、前記新グループ管理機器と前記グループ管理機器との間で、前記グループ管理機器に登録されていた元のメンバー機器を、前記グループ管理機器に登録するメンバー機器と、前記新グループ管理機器に登録するメンバー機器とに分ける選択手段と、前記新グループ管理機器が管理する新グループに固有の新共通秘密情報を、当該新グループ管理機器に選択された前記メンバー機器へ出力する通信手段とを備えるとしても良い。

【００５９】

また、前記グループ管理機器に登録されているメンバー機器はそれぞれ優先順位を付されており、前記取得手段は、他のメンバー機器の前記優先順位を取得し、前記選択手段は、取得した優先順位を基に、メンバー機器を分けるとしても良い。

この構成によると、一つのグループを複数のグループに分割することが出来る。

また、前記メンバー機器は、前記共通秘密情報を取得し、前記保持手段により保持した後に、更に、前記共通秘密情報を前記別のメンバー機器に出力する通信手段と、前記通信手段が前記共通秘密情報を出力すると、前記保持手段により保持されている共通秘密情報を削除する削除手段とを備えるとしても良い。

【００６０】

この構成によると、グループに登録したメンバー機器を交換することが出来る。また、他のメンバー機器に共通秘密情報を出力したメンバー機器は、前記共通秘密情報を削除するので、共通秘密情報を保持するメンバー機器、つまりグループに登録されているメンバー機器の台数を一定に保つことが出来る。

ここで、前記要求手段、取得手段及び保持手段は、前記メンバー機器に着脱可能な可搬型モジュールであり、前記可搬型モジュールは前記グループ管理機器に接続されると前記共通秘密情報を取得するとしても良い。

【００６１】

また、前記可搬型モジュールは、更に、前記保持手段が保持している前記共通秘密情報を前記メンバー機器へ通知する通知手段と、前記共通秘密情報を前記メンバー機器へ通知した後に、前記通知手段に対して前記共通秘密情報をメンバー機器へ更に通知することを禁止する管理手段とを備え、前記メンバー機器は、更に、前記可搬型モジュールから前記共通秘密情報を取得して格納する格納手段を備えるとしても良い。

【００６２】

この構成によると、ICカードが共通秘密情報を取得するので、グループ管理機器との通信機能を備えないメンバー機器でも、前記ICカードにより共通秘密情報を取得し、グループに登録することが出来る。

ここで、前記取得手段は、更に、コンテンツ鍵を用いて暗号化された暗号化コンテンツと、前記コンテンツ鍵を前記共通秘密情報を用いて生成された暗号化鍵を用いて暗号化して生成された暗号化コンテンツ鍵とを取得し、前記メンバー機器は、更に、接続された前記可搬型モジュールから前記共通秘密情報を読み出し、読み出した共通秘密情報から前記暗号化鍵と同一の復号鍵を生成し、生成した復号鍵を用いて前記暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、前記コンテンツ鍵を用いて前記暗号化コンテンツを復号する復号手段を備えるとしても良い。

【００６３】

この構成によると、メンバー機器は、ICカードが接続されている場合のみコンテンツを利用できる。また、ICカードが共通秘密情報を取得し、復号鍵を生成するため、任意の機器にICカードを接続し、グループ内の機器としてコンテンツを利用することが出来る。

ここで、前記保持手段は、更に、前記共通秘密情報を保持できる最大数を保持し、前記要求手段は、前記保持手段が保持する共通秘密情報の数が、前記最大数に満たない場合、前記グループ管理機器に、グループへの登録を要求するとしても良い。

【００６４】

また、前記保持手段は、更に、複数のグループを識別する識別子を保持し、前記要求手段は、前記識別子の何れか一つを付加して登録を要求し、前記保持手段は、前記共通秘密情報を、前記登録要求に含めて送信した識別子と対応付けて記憶するとしても良い。

この構成によると、メンバー機器は、複数の共通秘密情報を保持できるため、複数のグループに登録することが出来る。また、グループの識別子を付加して登録を要求すると、登録するグループを指定できる。

【００６５】

また、本発明は、メンバー機器をグループ管理機器に登録する登録機器であって、前記グループ管理機器からグループに固有の共通秘密情報を取得し、保持する保持手段と、前記メンバー機器に接続されると、当該メンバー機器に前記共通秘密情報を通知する通知手段とから構成されることを特徴とする登録機器である。

この構成によると、登録機器を用いることによって、グループ管理機器に接続できないメンバー機器でも、グループに登録することが出来る。

【００６６】

ここで、前記登録機器は、更に、前記共通秘密情報を前記メンバー機器へ通知した後に、前記通知手段に対して前記共通秘密情報をメンバー機器へ更に通知することを禁止する管理手段を備えるとしても良い。

この構成によると、メンバー機器へ共通秘密情報を通知すると、更に通知することを禁止するため、グループに登録する機器を制限台数以内に制限することが出来る。

【００６７】

ここで、前記登録機器は、更に、前記メンバー機器から、前記共通秘密情報の取得の要求を受け付ける受付手段を備え、前記通知手段は、前記要求を受け付けた場合に、前記共通秘密情報を通知するとしても良い。

この構成によると、共通秘密情報は登録機器が保持し、要求を受け付けた場合に、共通秘密情報を通知するため、任意の機器に登録機器を接続し、グループ内の機器としてコンテンツを利用することが出来る。また、メンバー機器は共通秘密情報を保持せず、登録装置が保持するので、グループ内の機器の台数を制限することが出来る。

【００６８】

また、本発明は、グループ管理機器に登録してコンテンツを利用するメンバー機器であって、前記グループ管理機器との距離、前記グループ管理機器との通信時間、前記グループ管理機器の処理能力又は前記グループ管理機器の処理状態のうち、予め設定された条件を基にして、複数のグループ管理機器から、１個のグループ管理機器を選択する選択手段と、選択したグループ管理機器に登録を要求する要求手段と、前記グループ管理機器から、グループ内で共通の共通秘密情報を取得する取得手段と、取得した共通秘密情報を保持する保持手段とから構成されることを特徴とするメンバー機器である。

【００６９】

この構成によると、メンバー機器は、グループ内に複数のグループ管理機器が存在する場合、複数のグループ管理機器のうち、比較的条件の良いグループ管理機器を選択し、当該グループ管理機器に登録することが出来る。

発明を実施するための最良の形態

以下、本発明の実施の形態について図面を用いて詳細に説明する。

１．グループ形成管理システム１の構成

グループ形成管理システム１は図１に示すように、AD内サーバ１００、再生装置２００、車載機器３００、ICカード４００及びＤＶＤ５００から構成される。

【００７０】

AD内サーバ１００及びモニタ２５１とスピーカ２５２とが接続されている再生装置２０

０は、ユーザ宅内に設置されており、オンラインで接続されている。車載機器３００は、ユーザが所有する車両に搭載されている。ICカード４００及びDVD５００は、AD内サーバ１００及び車載機器３００に接続可能である。ICカード４００はAD内サーバ１００に付属しており、AD内サーバ１００は、ICカード４００が接続されている場合のみ、動作する。

【００７１】

グループ形成管理システム１は、AD内サーバ１００が、コンテンツの利用が許可される範囲であるAD（Authorized Domain）を管理するシステムである。

AD内サーバ１００は、クライアント機器の登録を受け付けて管理し、AD内サーバ１００及び登録されたクライアント機器は、AD内サーバ１００により生成された共通秘密情報（以下CSI：Common Secret Information）を共有する。同一AD内の機器間では、共有したCSIを用いてお互いを認証し、認証に成功した場合にコンテンツの送受信やコピーを行う。前記CSIを持たない機器は、コンテンツの送受信やコピーを行うことは出来ない。

【００７２】

再生装置２００は、AD内サーバ１００と接続されているので、認証を行い、クライアント機器として登録することが出来る。また、車載機器３００は、AD内サーバ１００と接続されていないが、ICカード４００にCSIを記憶させ、ICカード４００から車載機器３００にCSIを通知することによってクライアント機器として登録することが出来る。

１．１　AD内サーバ１００の構成

AD内サーバ１００は図２に示すように、制御部１０１、秘密鍵格納部１０２、公開鍵証明書格納部１０３、CRL格納部１０４、公開鍵暗号処理部１０５、登録情報記憶部１０６、CSI生成部１０７、CSI格納部１０８、コンテンツ格納部１０９、暗号化部１１０、ID格納部１１１、ドライブ部１１２、入力部１１３、表示部１１４、入出力部１１５、入出力部１１６、復号部１１７及び暗号化部１１９から構成される。

【００７３】

AD内サーバ１００は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、AD内サーバ１００は、その機能を達成する。

【００７４】

AD内サーバ１００は、機器の登録、CSIの移動及び脱退の管理、コンテンツの配送及びコンテンツのコピーの処理を行う。

以下、各構成について説明する。

（１）入出力部１１５、１１６、ドライブ部１１２

入出力部１１５は、再生装置２００とデータの送受信を行う。入出力部１１６は、ＩＣカード４００が接続されたことを検出すると、制御部１０１に検出を出力する。また、ICカード４００とデータの送受信を行う。ドライブ部１１２は、DVD５００へデータの書き込み、読み出しを行う。

（２）秘密鍵格納部１０２、公開鍵証明書格納部１０３、CRL格納部１０４、コンテンツ格納部１０９、ID格納部１１１、コンテンツ鍵格納部１１８

ID格納部１１１は、AD内サーバ１００に固有のIDであるID#1を記憶している。

【００７５】

公開鍵証明書格納部１０３は、公開鍵証明書Cert#1を格納する。

公開鍵証明書Cert#1は、公開鍵PK#1がAD内サーバ１００の正しい公開鍵であることを証明するものである。公開鍵証明書Cert#1は、署名データSig#CA1、公開鍵PK#1及びID#1を含む。署名データSig#CA1は、CA（Certification Authority）により、AD内サーバ１００の公開鍵PK#1及びID#1に対して署名アルゴリズムSを施して生成した署名データである。ここでCAとは、信頼できる第三者機関であり、グループ形成管理システム１に属する機器の公開鍵の正当性を証明する公開鍵証明書を発行する機関である。なお、署名アルゴリズムSは、一例として、有限体上のＥｌＧａｍａｌ署名である。ＥｌＧａｍａｌ署名につい

ては、公知であるので説明を省略する。

【００７６】

秘密鍵格納部１０２は、外部から内部を見ることが出来ない耐タンパ領域であり、公開鍵PK#1に対応する秘密鍵SK#1を格納する。

CRL格納部１０４は、CRL（Certification Revocation List）を格納する。このCRLは、不正を行った機器や、秘密鍵が暴露された機器など、無効化された機器のIDが登録されたリストであり、CAから発行される。なお、CRLに登録されるのは、機器のIDでなくてもよく、無効化された機器が有する公開鍵証明書のシリアル番号が登録されるとしても良い。CRLは、放送、インターネット又はDVD等の記録媒体に記録されて各機器へ配布され、各機器は、最新のCRLを入手する。なお、CRLについては、「American National Standards Institute, American National Standard for financial Services,ANSX9.57:Public Key Cryptography For the Financial Industry: Certificate Management,1997.」に詳しく開示されている。

【００７７】

コンテンツ格納部１０９は、コンテンツ鍵を用いて暗号化された暗号化コンテンツを格納する。なお、コンテンツの取得方法は、本発明の主題ではないので、説明を省略するが、例として、インターネット、放送などを利用して取得する方法や、DVD等の記録媒体から取得する方法が有る。

コンテンツ鍵格納部１１８は、暗号化部１１０から暗号化コンテンツ鍵ａを受け取り、格納する。

（３）公開鍵暗号処理部１０５

公開鍵暗号処理部１０５は、他の機器と通信する際に、認証を行い、SAC（Secure Authentication Channel）を確立する。SACとは、暗号通信が可能となる安全な通信路を意味する。SACを確立する処理によって、認証相手の機器がCAに認められた正しい機器であることを確認できる。詳しい確立方法については後述する。また、公開鍵暗号処理部１０５は、認証によって、セッション鍵SKを共有する。

（４）登録情報記憶部１０６

登録情報記憶部１０６は、耐タンパ領域であり、図３（ａ）に示す登録情報を記憶している。登録情報は、AD内サーバ１００に登録可能な機器の台数及び登録されている機器のIDを管理する情報であり、機器ID、最大、登録台数、残数及びICカードIDから構成される。

【００７８】

機器IDは、AD内サーバ１００に登録された機器のIDを記憶する領域である。AD内サーバ１００に再生装置２００及び車載機器３００が登録されると、図３（ｂ）のように、それぞれのＩＤであるID#2及びID#3が格納される。

最大は、AD内サーバ１００に登録可能な機器の最大数を示し、本実施の形態では、２台である。登録台数は、既にAD内サーバ１００に登録されている機器の台数を示す。残数は、AD内サーバ１００に登録可能な台数を示す。

【００７９】

AD内サーバ１００にクライアント機器が登録されていない初期の状態では、登録台数は「０」であり、残数は最大と同数である。AD内サーバ１００に何れかのクライアント機器が登録されると、登録台数に「１」が加算され、残数から「１」が減算される。

ICカードIDは、AD内サーバ１００に付属のICカード４００のIDを予め記憶しており、書き換え出来ない。

（５）CSI生成部１０７、CSI格納部１０８

CSI格納部１０８は、外部からCSIを読むことが出来ない耐タンパ領域であり、AD内サーバ１００に機器が登録されていない場合、未登録であることを示す値として「０」を記憶している。

【００８０】

CSI生成部１０７は、制御部１０１の制御の基、AD内サーバ１００に最初に機器を登録

する際に、CSIを生成する。また、登録した機器が全て脱退すると、CSI格納部１０８は、格納している値を「０」に書き換える。

ここでCSIは、CSI生成部１０７によって生成される任意のデータであり、本実施の形態では２００ビットとする。なお、CSIのビット長は、これに限定されず、容易に推測されない、簡単に試すことが不可能な程度の長さであれば良い。

【００８１】

CSI生成部１０７は生成したCSIをCSI格納部１０８に格納する。また、生成したCSIを、接続されているICカード４００に出力する。

なお、CSIは、定期的又は不定期に更新するとしても良い。

（６）暗号化部１１０，１１９

暗号化部１１９は、再生装置２００の登録の際、制御部１０１の制御の基、公開鍵暗号処理部１０５から受け取るセッション鍵SKを用いて、CSIに暗号化アルゴリズムEを施して暗号化CSIを生成し、生成した暗号化CSIを入出力部１１５を介して再生装置２００へ送信する。ここで、暗号化アルゴリズムSは、一例としてDESである。DESについては公知であるので、説明を省略する。

【００８２】

暗号化部１１０は、コンテンツ鍵をコンテンツ鍵格納部１１８に格納する際、ID格納部１１１からID#1を読み出し、CSI格納部１０４からCSIを読み出す。読み出したID#1及びCSIをこの順で連結して暗号鍵ａとし、暗号鍵ａを用いてコンテンツ鍵に暗号化アルゴリズムEを施して暗号化して暗号化コンテンツ鍵ａを生成し、生成した暗号化コンテンツ鍵ａをコンテンツ鍵格納部１１８へ格納する。

【００８３】

暗号化部１１０は、ＤＶＤ５００に暗号化コンテンツを書き込む際、制御部１０１の制御の基、登録情報記憶部１０６から登録情報の機器ＩＤから登録されている機器のＩＤであるID#2及びID#3を読み出す。ID#２とCSIとをこの順で連結し、暗号鍵ｂとし、ID#3とCSIとをこの順で連結して、暗号鍵ｃとする。暗号鍵ｂ及び暗号鍵ｃをそれぞれ用いて暗号化コンテンツ鍵ｂ及び暗号化コンテンツ鍵ｃを生成し、DVD５００に書き込む。

（７）復号部１１７

復号部１１７は、制御部１０１の制御の基、ID格納部１１１に記憶しているID#１を読み出し、CSI格納部１０８に格納しているCSIを読み出す。ID#1及びCSIをこの順で連結して復号鍵として用い、コンテンツ鍵格納部１１８から読み出した暗号化コンテンツ鍵ａに復号アルゴリズムDを施し、コンテンツ鍵を生成する。生成したコンテンツ鍵は、暗号化部１１０へ出力する。ここで、復号アルゴリズムDとは、暗号化アルゴリズムEの逆の処理をするアルゴリズムである。

（８）制御部１０１、入力部１１３、表示部１１４

入力部１１３は、ユーザからの入力を受け付け、受け付けた入力を制御部１０１へ出力する。

【００８４】

制御部１０１は、処理を開始する際、接続されているICカード４００からICカードのIDを受信すると、受信したIDが登録情報のICカードＩＤと一致するか否かを確認する。一致しない場合は、接続されたICカードが付属のICカードでないことを表示部１１４に表示し、処理を終了する。一致する場合のみ、以降の処理を継続する。

＜再生装置２００の登録＞

再生装置２００から入出力部１１５を介して登録要求を受け取ると、制御部１０１は、公開鍵暗号処理部１０５を制御し、CSIの初期値「０」を用いて後述の方法でSACを確立する。ここで、登録の際の認証に使用する「０」は、再生装置２００が、何れのＡＤにも登録されていないことを示す。SACを確立する際の機器認証の結果から、相手機器が未登録であるか否かを判断する。認証相手の機器が保持するCSIの値が「０」である場合、認証に成功し、未登録であると判断する。認証相手の機器が保持するCSIの値が、「０」でない場合、制御部１０１は、相手の機器が既に何れかのADに登録されていると判断する。

【００８５】
未登録であると判断した場合、登録情報記憶部１０６から登録情報を読み出し、残数が「０」であるか否かを判断する。残数が「０」でない場合、登録台数が「０」か否かを判断する。登録台数が「０」の場合、CSI生成部１０７を制御してCSIを生成し、CSI格納部１０８へ格納する。登録台数が「０」でなかった場合は、CSI格納部１０８からCSIを読み出し、生成又は読み出したCSIを暗号化部１１０で暗号化して生成した暗号化CSIを入出力部１１５を介して、再生装置２００へ出力する。再生装置２００から、CSIを受け取った事を示す受領通知を受信すると、登録情報の登録台数に「１」を加算し、残数から「１」を減算し、処理を終了する。

【００８６】
機器認証の結果が失敗の場合、相手機器が登録済みである場合及び残数が「０」である場合は、登録できないことを示す登録不可通知を再生装置２００へ送信し、処理を終了する。

また、CSI生成部１０７でCSIを生成する際、ICカード４００との間でSACを確立してセッション鍵SKを共有し、セッション鍵SKを用いて生成したCSIに暗号化アルゴリズムEを施して暗号化CSIを生成し、生成した暗号化CSIをICカード４００へ送信する。

【００８７】
なお、上記登録処理の認証において、認証相手のクライアント機器のCSIが、CSI格納部１０８に格納しているCSIと一致するか否かを確認することによって、AD内サーバ１００が管理するADに登録済みか否かを判断しても良い。クライアント機器の保持するCSIが、CSI格納部１０８に格納しているCSIと一致する場合、クライアント機器に対して、既にAD内サーバ１００に登録している旨を通知した後、登録の処理を終了するとしても良い。

【００８８】
また、クライアント機器が保持するCSIが、「０」でなく、CSI格納部１０８に格納しているCSIと異なる場合、他のADに登録されていると判断する。クライアント機器が他のADに登録されていると判断する場合、上記登録不可通知を送信後、登録の処理を終了するとしても良い。また、他のADに登録済みであることを通知し、更にAD内サーバ１００への登録を続行するかを尋ね、続行する場合は、上記登録の処理を続行して、CSI格納部１０８に格納しているCSIを送信するとしても良い。この場合、クライアント機器は、AD内サーバ１００からCSIを受信すると、他のADのCSIに、受信したCSIを上書きする。

【００８９】
また、上記登録処理の認証において、クライアント機器を不正な機器でないと判断した場合、クライアント機器が保持するCSIが如何なる値であっても登録処理を行い、CSIを送信するとしても良い。

＜車載機器３００の登録＞
（ａ）既にIDを確認済みのICカード４００が接続された状態で、入力部１１３から、CSIをコピーする旨の入力を受け付けると、制御部１０１は、残数が「０」か否かを判断し、「０」でなければ、ICカード４００に、CSIのコピーを１回許可することを示す許可権利を送信する。制御部１０１は、ICカード４００から受領通知を受け取ると、処理を終了する。

【００９０】
残数が「０」の場合は、表示部１１４にコピーできない旨を表示し、処理を終了する。
（ｂ）ICカード４００が接続され、IDを確認し、CSIをコピーしたことを示すコピー通知を受け取ると、コピー通知に含まれる、CSIのコピー先のIDを抽出し、登録情報に機器IDとして記憶する。また、ICカード４００へ、コピー先のIDを受け取ったことを示す受領通知を送信する。

【００９１】
なお、ここでは、既にCSIが生成されているものとして説明したが、CSIが生成されていない場合は、前述の再生装置２００を登録する際と同様に生成してICカード４００へ送信する。

＜コンテンツ配布＞

入出力部１１５を介して再生装置２００からコンテンツの配送要求を受信すると、制御部１０１は公開鍵暗号処理部１０５を制御して後述の方法でSACを確立し、セッション鍵SKを共有する。このSAC確立の際の認証では、CSI格納部１０８が格納しているCSIを用いるため、認証に成功した場合、相手機器はAD内サーバ１００が生成したCSIを保持しているので、登録済みであると判断し、認証に失敗した場合、AD内サーバ１００に登録されていないと判断する。

【００９２】

認証に失敗した場合、コンテンツを配送できないことを示す配送不可通知を再生装置２００へ送信する。

認証に成功した場合、復号部１１７を制御して、コンテンツ鍵格納部１１８に格納している暗号化コンテンツ鍵ａを復号する。次に暗号化部１１９を制御して、セッション鍵SKを用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵ｓを生成させ、再生装置２００へ送信する。また、コンテンツ格納部１０９から暗号化コンテンツを読み出し、再生装置２００へ送信する。

＜コンテンツをDVDに記録＞

入力部１１３からコンテンツをDVD５００に記録する旨の入力を受け付けると、復号部１１７を制御してコンテンツ鍵格納部１１８に格納している暗号化コンテンツ鍵ａを復号させてコンテンツ鍵を生成させる。次に、暗号化部１１９を制御して登録情報に登録しているID#２及びID#３をそれぞれ用いて生成した暗号鍵ｂ及び暗号鍵ｃを用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵ｂ及び暗号化コンテンツ鍵ｃを生成し、生成した暗号化コンテンツ鍵ｂ及びｃをDVD５００へ書き込む。また、コンテンツ格納部１０９から暗号化コンテンツを読み出し、DVD５００へ書き込む。

【００９３】

なお、DVD５００に固有のIDを基にして生成した暗号化鍵又はDVD５００に固有のID及びCSIを基にして生成した暗号化鍵を用いて、コンテンツ鍵を暗号化するとしても良い。

＜脱退＞

再生装置２００からID#2を含む脱退要求を受け取ると、公開鍵暗号処理部１０５を制御して後述の方法でSACを確立する。この際、CSI格納部１０８に格納しているCSIを用いて認証を行う。SAC確立の際の認証結果から、要求元の機器が登録済みであるか否かを判断し、未登録の場合脱退できないので、再生装置２００へ未登録であることを示す未登録通知を送信する。

【００９４】

登録済みの場合、再生装置２００へCSIを削除することを示す削除通知を送信する。再生装置２００からCSIの削除が完了したことを示す完了通知を受信すると、登録情報の機器IDからID#2を削除し、登録台数から「１」減算し、残数に「１」を加算する。

１．２　再生装置２００の構成

再生装置２００は、図４に示すように、制御部２０１、秘密鍵格納部２０２、公開鍵証明書格納部２０３、CRL格納部２０４、公開鍵暗号処理部２０５、CSI格納部２０８、コンテンツ格納部２０９、ID格納部２１１、入力部２１３、入出力部２１５、復号部２１７、暗号化部２１８、コンテンツ鍵格納部２１９、復号部２２０及び再生部２２１から構成される。再生部２２１には、モニタ２５１及びスピーカ２５２が接続されている。

【００９５】

再生装置２００は、AD内サーバ１００と同様のコンピュータシステムであり、ＲＡＭ又はハードディスクユニットには、コンピュータプログラムが記憶されている。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、再生装置２００は、その機能を達成する。

（１）入出力部２１５

入出力部２１５は、AD内サーバ１００とデータの送受信を行う。

（２）秘密鍵格納部２０２、公開鍵証明書格納部２０３、CRL格納部２０４、CSI格納部２

０８、ID格納部２１１
CRL格納部２０４は、最新のCRLを格納している。
【００９６】
ID格納部２１１は、再生装置２００に固有のIDであるID#2を記憶している。
CSI格納部２０８は、耐タンパ領域であり、未登録であることを示す「０」を格納している。AD内サーバ１００に登録されると、AD内サーバ１００より取得したCSIを格納する。
公開鍵証明書格納部２０３は、CAより発行された公開鍵証明書Cert#2を格納する。この公開鍵証明書Cert#2は、再生装置２００の公開鍵PK#2及び再生装置２００のID#２と、それらに対するCAの署名データSig#CA2とを含む。
【００９７】
秘密鍵格納部２０２は、耐タンパ領域であり、再生装置２００の公開鍵PK#2と対応する秘密鍵SK#2を格納する。
（３）公開鍵暗号処理部２０５
公開鍵暗号処理部２０５は、AD内サーバ１００と通信する際に、後述の方法でSACを確立し、セッション鍵SKを共有する。共有したセッション鍵SKを、復号部２１７へ出力する。
（４）復号部２１７、復号部２２０
復号部２１７は、AD内サーバ１００からコンテンツを配送される際、公開鍵暗号処理部２０５で共有したセッション鍵SKを用いて、AD内サーバ１００より配信された暗号化コンテンツ鍵ｓに、復号アルゴリズムDを施してコンテンツ鍵を生成する。ここで、復号アルゴリズムDとは、暗号化アルゴリズムEと逆の処理を行う。
【００９８】
また、一旦格納したコンテンツを再生する際、ID格納部２１１からID#2を読み出し、CSI格納部２０８からCSIを読み出し、ID#2及びCSIをこの順で連結して復号鍵ｂを生成する。生成した復号鍵ｂを用いて、コンテンツ鍵格納部２１９から読み出した暗号化コンテンツ鍵ｂに、復号アルゴリズムDを施してコンテンツ鍵を生成し、生成したコンテンツ鍵を復号部２２０へ出力する。
【００９９】
復号部２２０は、コンテンツ格納部２０９に格納されている暗号化コンテンツを読み出し、復号部２１７から受け取るコンテンツ鍵を用いて、読み出した暗号化コンテンツに復号アルゴリズムDを施してコンテンツを生成し、生成したコンテンツを再生部２２１へ出力する。
（５）暗号化部２１８
暗号化部２１８は、AD内サーバ１００から取得したコンテンツを格納する際、ID格納部２１１からID#2を読み出し、CSI格納部２０８からCSIを読み出す。ID#2及びCSIをこの順で連結して暗号鍵ｂを生成し、生成した暗号鍵ｂを用いて復号部２１７から受け取るコンテンツ鍵に暗号化アルゴリズムEを施して暗号化コンテンツ鍵ｂを生成し、生成した暗号化コンテンツ鍵ｂをコンテンツ鍵格納部２１９に出力する。
（６）コンテンツ格納部２０９、コンテンツ鍵格納部２１９
コンテンツ格納部２０９は、AD内サーバ１００から送信される暗号化コンテンツを格納する。
【０１００】
コンテンツ鍵格納部２１９は、暗号化部２１８で暗号化された暗号化コンテンツ鍵ｂを格納する。
（７）制御部２０１、入力部２１３
＜登録＞
入力部２１３が登録処理を開始する旨の入力を受け付けると、制御部２０１は、ID格納部２１１からID#2を読み出し、ID#2を含めた登録要求を、入出力部２１５を介して、AD内サーバ１００へ送信し、後述の方法でSACを確立する。

【０１０１】
制御部２０１は、AD内サーバ１００から、登録不可通知を受信すると、モニタ２５１に登録できない旨を表示し、登録の処理を終了する。
制御部２０１は、AD内サーバ１００から暗号化CSIを受信すると、復号部２１７を制御して復号させてCSIを生成し、生成したCSIをCSI格納部２０８に格納する。また、CSIを受領したことを示す受領通知をAD内サーバ１００へ送信する。
＜コンテンツの配送＞
入力部２１３がコンテンツを取得して再生する旨の入力を受け付けると、制御部２０１は、配送要求をAD内サーバ１００へ送信する。
【０１０２】
制御部２０１は、AD内サーバ１００から配送不可通知を受信すると、モニタ２５１に配送できない旨を表示し、処理を終了する。
受信したコンテンツを再生する場合、制御部２０１は、AD内サーバ１００から暗号化コンテンツ鍵ｓを受信すると、復号部２１７を制御して復号させてコンテンツ鍵を生成させる。また、AD内サーバ１００から暗号化コンテンツを受信すると、復号部２２０を制御し、暗号化コンテンツを復号してコンテンツを生成させ、再生部２２１にコンテンツを再生させる。
＜コンテンツを蓄積してから再生＞
入力部２１３がコンテンツを取得して蓄積する旨の入力を受け付けると、制御部２０１は、上記と同様に処理してコンテンツを取得する。コンテンツを取得すると、制御部２０１は、AD内サーバ１００から受信した暗号化コンテンツ鍵ｓを復号部２１７に復号させ、復号したコンテンツ鍵を暗号化部２１８を制御して暗号化させ、暗号化コンテンツ鍵ｂとしてコンテンツ鍵格納部２１９に格納する。また、AD内サーバ１００から暗号化コンテンツを受信すると、コンテンツ格納部２０９に格納する。
【０１０３】
入力部２１３がコンテンツ格納部２０９に格納したコンテンツを再生する旨の入力を受け付けると、制御部２０１は、復号部２１７を制御して暗号化コンテンツ鍵ｂを復号させ、復号部２２０に暗号化コンテンツを復号させてコンテンツを生成し、再生部２２１にコンテンツを再生させる。
＜脱退＞
入力部２１３が脱退処理を開始する旨の入力を受け付けると、制御部１０１は、後述の方法でSACを確立する。
【０１０４】
制御部２０１は、AD内サーバ１００から未登録通知を受信すると、AD内サーバ１００に登録されていないことをモニタ２５１に表示して処理を終了する。
制御部２０１は、AD内サーバ１００から削除通知を受信すると、CSI格納部２０８に格納しているCSIを削除し、未登録を示す「０」を格納する。また、削除が完了したことをAD内サーバ１００に通知する削除完了通知を送信する。
（８）再生部２２１
再生部２２１は、復号部２２０から受け取るコンテンツから映像信号を生成し、生成した映像信号をモニタ２５１へ出力する。また、受け取ったコンテンツから音声信号を生成し、生成した音声信号をスピーカ２５２へ出力する。
１．３　車載機器３００の構成
車載機器３００は図５に示すように、制御部３０１、秘密鍵格納部３０２、公開鍵証明書格納部３０３、CRL格納部３０４、公開鍵暗号処理部３０５、CSI格納部３０８、ID格納部３１１、ドライブ部３１２、入力部３１３、入出力部３１６、復号部３１７、３１８、３２０、再生部３２１、モニタ３２２及びスピーカ３２３から構成される。
【０１０５】
車載機器３００は、AD内サーバ１００と同様のコンピュータシステムであり、ＲＡＭ又はハードディスクユニットには、コンピュータプログラムが記憶されている。マイクロプ

ロセッサが、コンピュータプログラムに従って動作することにより、車載機器３００は、その機能を達成する。

（１）ドライブ部３１２、入出力部３１６

ドライブ部３１２は、DVD５００から暗号化コンテンツ鍵ｃを読み出し、復号部３１８へ出力する。また、暗号化コンテンツを読み出し、復号部３２０へ出力する。

【０１０６】

入出力部３１６は、制御部３０１の制御の基、ICカード４００とデータの送受信を行う。

（２）秘密鍵格納部３０２、公開鍵証明書格納部３０３、CRL格納部３０４、CSI格納部３０８、ID格納部３１１

CRL格納部３０４は、最新のCRLを格納する。

【０１０７】

ID格納部３１１は、車載機器３００に固有のIDであるID#3を記憶している。

CSI格納部３０８は、耐タンパ領域であり、未登録を示す「０」を格納している。ICカード４００から、AD内サーバ１００により生成されたCSIを受け取ると、受け取ったCSIを格納する。

公開鍵証明書格納部３０３は、CAより発行された公開鍵証明書Cert#3を格納する。この公開鍵証明書Cert#3は、車載機器３００の公開鍵PK#3及びID#3と、それらに対するCAの署名データSig#CA3とを含む。

【０１０８】

秘密鍵格納部３０２は、耐タンパ領域であり、公開鍵PK#3と対応する秘密鍵SK#3を格納している。

（３）公開鍵暗号処理部３０５

公開鍵暗号処理部３０５は、制御部３０１の制御の基、ICカード４００と認証を行い、後述の方法でSACを確立する。また、この際に共有したセッション鍵SKを復号部３１７へ出力する。

（４）復号部３１７，３１８，３２０

復号部３１７は、制御部３０１の制御の基、ICカード４００から暗号化CSIを受け取ると、公開鍵暗号処理部３０５から受け取るセッション鍵SKを用いて、暗号化CSIに復号アルゴリズムDを施してCSIを生成し、生成したCSIをCSI格納部３０８へ出力する。

【０１０９】

復号部３１８は、コンテンツを再生する際、ドライブ部から暗号化コンテンツ鍵ｃを受け取ると、ID格納部３１１からID#3を読み出し、CSI格納部３０８からCSIを読み出す。読み出したID#3及びCSIをこの順で連結して復号鍵ｃを生成する。復号鍵ｃを用いて暗号化コンテンツ鍵ｃに復号アルゴリズムDを施してコンテンツ鍵を生成し、生成したコンテンツ鍵を復号部３２０へ出力する。

【０１１０】

復号部３２０は、ドライブ部３１２から暗号化コンテンツを受け取り、復号部３１８からコンテンツ鍵を受け取る。受け取ったコンテンツ鍵を用いて暗号化コンテンツに復号アルゴリズムDを施してコンテンツを生成し、生成したコンテンツを再生部３２１へ出力する。

（５）制御部３０１、入力部３１３

制御部３０１は、ICカード４００が接続されると、SACを確立する。この際、CSI格納部３０８に格納されている「０」をCSIとして用いる。機器認証に失敗した場合、処理を終了する。また、ICカード４００から登録済通知を受け取った場合、登録済みであることをモニタ３２２に表示して処理を終了する。制御部３０１は、入出力部３１６を介してICカード４００から暗号化CSIを受け取ると、復号部３１７を制御して復号させてCSIを生成し、生成したCSIをCSI格納部３０８に格納する。また、CSIを受領したことを示す受領通知をICカード４００へ送信する。

【０１１１】

なお、車載機器３００から他の機器へのCSIのコピーは行わない。

制御部３０１は、入力部３１３からDVD５００に記録されているコンテンツを視聴する旨の入力を受け付けると、ドライブ部３１２を制御してDVD５００から暗号化コンテンツ鍵ｃ及び暗号化コンテンツを読み出す。復号部３１８で暗号化コンテンツ鍵ｃを復号させてコンテンツ鍵を生成させ、復号部３２０で暗号化コンテンツを復号させてコンテンツを生成させる。また、再生部３２１を制御してコンテンツを再生させる。

（６）再生部３２１、モニタ３２２、スピーカ３２３

再生部３２１は、受け取ったコンテンツから映像信号を生成してモニタ３２２へ出力し、音声信号を生成してスピーカ３２３へ出力し、コンテンツを再生する。

１．４　ICカード４００の構成

ICカード４００は図６に示すように、制御部４０１、秘密鍵格納部４０２、公開鍵証明書格納部４０３、CRL格納部４０４、公開鍵暗号処理部４０５、CSI格納部４０８、ID格納部４１１、入出力部４１６、復号部４１７、暗号化部４１８及びID記憶部４２０から構成される。

【０１１２】

ICカード４００は、AD内サーバ１００及び車載機器３００に接続可能である。車載機器３００のような、AD内サーバ１００と接続できない機器をAD内の機器として登録する際に用いる。

（１）秘密鍵格納部４０２、公開鍵証明書格納部４０３、CRL格納部４０４、CSI格納部４０８、ID格納部４１１、ID記憶部４２０

CRL格納部４０４は、最新のCRLを格納する。

【０１１３】

ID格納部４１１は、ICカード４００に固有のIDであるID#4を記憶している。

CSI格納部４０８は、耐タンパ領域であり、AD内サーバ１００にクライアント機器が登録されていない場合、未登録を示す「０」を格納している。AD内サーバ１００によりCSIが生成されると、AD内サーバ１００より取得したCSIと、コピー回数である「０」とを対応付けて記憶する。ここで、コピー回数とは、他のクライアント機器へCSIを通知することを許可された回数である。

【０１１４】

公開鍵証明書格納部４０３は、CAより発行された公開鍵証明書Cert#4を格納する。この公開鍵証明書Cert#4は、ICカード４００の公開鍵PK#4及びID#4と、それらに対するCAの署名データSig#CA4とを含む。

秘密鍵格納部４０２は、耐タンパ領域であり、公開鍵PK#4と対応する秘密鍵SK#4を格納している。

【０１１５】

ID記憶部４２０は、CSIのコピー先のIDを記憶する領域である。

（２）公開鍵暗号処理部４０５

公開鍵暗号処理部４０５は、制御部４０１の制御の基、AD内サーバ１００とSACを確立し、セッション鍵SKを共有し、共有したセッション鍵SKを復号部４１７へ出力する。

また、車載機器３００との間にSACを確立してセッション鍵SKを共有し、共有したセッション鍵SKを暗号化部４１８へ出力する。

（３）復号部４１７

復号部４１７は、入出力部４１６を介して暗号化CSIを受け取ると、制御部４０１の制御の基、公開鍵暗号処理部４０５から受け取るセッション鍵SKを用いて暗号化CSIに復号アルゴリズムDを施してCSIを生成する。生成したCSIをCSI格納部４０８へ格納する。

（４）暗号化部４１８

暗号化部４１８は、制御部４０１の制御の基、CSI格納部４０８からCSIを読み出し、公開鍵暗号処理部４０５からセッション鍵SKを受け取り、セッション鍵SKを用いてCSIに暗号化アルゴリズムEを施して暗号化CSIを生成し、生成した暗号化CSIを車載機器３００へ送信する。

（５）制御部４０１、入出力部４１６

AD内サーバ１００に接続されると、制御部４０１は、ID格納部４１１からID#4を読み出し、読み出したID#4をAD内サーバ１００へ送信する。

【０１１６】

AD内サーバ１００からCSIを受け取る際、制御部４０１は、公開鍵暗号処理部４０５を制御してAD内サーバ１００との間にSACを確立してセッション鍵SKを共有し、暗号化CSIを受信すると、復号部４１７で復号させてCSIを生成し、CSI格納部４０８にCSIを格納する。

車載機器３００を登録する際、制御部４０１は、AD内サーバ１００から許可権利を受信すると、CSIと対応付けて格納しているコピー回数に「１」を加算し、AD内サーバ１００に、受領通知を送信する。

【０１１７】

車載機器３００に接続されると、公開鍵暗号処理部４０５を制御してSACを確立し、セッション鍵SKを共有する。この際、CSIとして初期値「０」を用いて認証を行い、認証結果から、車載機器３００が未登録であるか否かを判断する。認証が失敗の場合、登録済みであると判断し、登録済通知を送信し、処理を終了する。認証か成功の場合、未登録であると判断し、認証の際に受け取る、車載機器３００のID#3をID記憶部４２０に記憶する。制御部４０１は、CSI格納部４０８に格納しているCSIを読み出し、暗号化部４１８で暗号化して暗号化CSIを生成し、車載機器３００へ送信する。制御部４０１は、車載機器３００から受領通知を受け取ると、コピー回数から「１」減算し、処理を終了する。

【０１１８】

制御部４０１は、AD内サーバ１００に接続されると、ID格納部４１１からID#4を読み出してAD内サーバ１００へ送信する。また、ID記憶部４２０からCSIのコピー先のIDを読み出し、読み出したIDを含むコピー通知をAD内サーバ１００へ送信する。AD内サーバ１００から受領通知を受け取ると、処理を終了する。

２．グループ形成管理システム１の動作

２．１　ＳＡＣの動作

SACを確立する際の動作について、図７，８を用いて説明する。

【０１１９】

なお、このSACの確立方法は、AD内サーバ１００、再生装置２００、車載機器３００及びＩＣカード４００の何れの機器同士の認証にも利用するため、ここでは認証を行う機器を、機器A及び機器Bと称する。また、認証で使用するCSIは、未登録を示す「０」の場合と、AD内サーバ１００が生成した値の場合とが有るが、ここでは全てCSIとして説明する。

【０１２０】

ここで、Gen()を鍵生成関数とし、Yを、システム固有のパラメータとする。また、鍵生成関数Gen()は、Gen(ｘ、Gen(y,z))＝Gen(y,Gen(x,z))の関係を満たすものとする。なお、鍵生成関数は、任意の公知技術で実現可能なため、その詳細についてここでは言及しない。その一例として、文献（１）池野信一、小山謙二、「現代暗号理論」、電気通信学会にディフィーヘルマン（DH）型公開鍵配送法が開示されている。

【０１２１】

機器Aは、公開鍵証明書Cert#Aを読み出し（ステップＳ１１）、機器Bへ送信する（ステップＳ１２）。

公開鍵証明書Cert#Aを受け取った機器Bは、CAの公開鍵PK#CAを用いて、公開鍵証明書Cert#Aに含まれる署名データSig#CAに対して、署名検証アルゴリズムVを施して署名検証する（ステップＳ１３）。検証結果が失敗の場合（ステップＳ１４でNO）、処理を終了する。検証結果が成功の場合（ステップＳ１４でYES）、CRLを読み出し（ステップＳ１５）、公開鍵証明書Cert#Aに含まれて受け取ったID#AがCRLに登録されているか否かを判断する（ステップＳ１６）。登録されていると判断する場合（ステップＳ１６でYES）、処理を終了する。登録されていないと判断する場合（ステップＳ１６でNO）、機器Bの公開鍵証

明書Cert#Bを読み出し（ステップＳ１７）、機器Aへ送信する（ステップＳ１８）。

【０１２２】

機器Aは、公開鍵証明書Cert#Bを受け取ると、公開鍵PK#CAを用いて公開鍵証明書Cert#Bに含まれる署名データSig#CAに対して、署名検証アルゴリズムVを施して署名検証する（ステップＳ１９）。検証結果が失敗の場合（ステップＳ２０でNO）、処理を終了する。検証結果が成功の場合（ステップＳ２０YES）、CRLを読み出し（ステップＳ２１）、公開鍵証明書Cert#Bに含まれて受け取ったID#BがCRLに登録されているか否かを判断する（ステップＳ２２）。登録されていると判断する場合（ステップＳ２２でYES）、処理を終了する。登録されていないと判断する場合（ステップＳ２２でNO）、処理を継続する。

【０１２３】

機器Bは、乱数Cha#Bを生成し（ステップＳ２３）、機器Aへ送信する（ステップＳ２４）。

機器Aは、乱数Cha#Bを受け取ると、Cha#BとCSIとをこの順で連結してCha_B||CSIを生成し（ステップＳ２５）、生成したCha_B||CSIに、機器Aの秘密鍵SK#Aを用いて署名生成アルゴリズムSを施して署名データSig#Aを生成し（ステップＳ２６）、生成した署名データSig#Aを機器Bへ送信する（ステップＳ２７）。

【０１２４】

機器Bは、署名データSig#Aを受け取ると、ステップＳ１２でCert#Aに含んで受け取ったPK#Aを用いて受け取った署名データSig#Aに署名検証アルゴリズムVを施して署名検証し（ステップＳ２８）、検証結果が失敗の場合は（ステップＳ２９でNO）、処理を終了し、成功の場合（ステップＳ２９でYES）は処理を継続する。

機器Aは、乱数Cha#Aを生成し（ステップＳ３０）、機器Bへ送信する（ステップＳ３１）。

【０１２５】

機器Bは、受け取ったCha#AとCSIとをこの順で連結してCha#A||CSIを生成し（ステップＳ３２）、生成したCha#A||CSIに、機器Bの秘密鍵SK#Bを用いて署名生成アルゴリズムSを施して署名データSig#Bを生成し（ステップＳ３３）、生成した署名データSig#Bを機器Aへ送信する（ステップＳ３４）。

機器Aは、署名データSig#Bを受け取ると、ステップＳ１８でCert#Bに含んで受け取ったPK#Bを用いて署名データSig#Bに署名検証アルゴリズムVを施して署名検証し（ステップＳ３５）、検証結果が失敗の場合（ステップＳ３６でNO）、処理を終了する。成功の場合（ステップＳ３６でYES）、乱数「ａ」を生成し（ステップＳ３７）、生成した「ａ」を用いてKey#A＝Gen(a,Y)を生成し（ステップＳ３８）、生成したKey#Aを機器Bへ送信する（ステップＳ３９）。

【０１２６】

機器Bは、Key#Aを受け取ると、乱数「ｂ」を生成し（ステップＳ４０）、生成した乱数「ｂ」を用いてKey#B＝Gen(b,Y)を生成する（ステップＳ４１）。生成したKey#Bを機器Aへ送信する（ステップＳ４２）。また、生成した乱数「ｂ」と、受け取ったKey#Aとを用いて、Key#AB＝Gen(b,Key#A)＝Gen(b,Gen(a,Y))を生成し（ステップＳ４３）、Key#ABと、CSIとを用いてセッション鍵SK＝Gen(CSI,Key#AB)を生成する（ステップＳ４４）。

【０１２７】

機器Aは、Key#Bを受け取ると、生成した乱数「ａ」と受け取ったKey#BとからKey#AB＝Gen(a,Key#B)＝Gen(a,Gen(b,y))を生成し（ステップＳ４５）、生成したKey#ABとCSIとを用いて、セッション鍵SK＝Gen(CSI,Key#AB)を生成する（ステップＳ４６）。

２．２　再生装置２００登録の動作

ＡＤ内サーバ１００に、再生装置２００を登録する際の動作を図９を用いて説明する。

【０１２８】

なお、AD内サーバ１００は、ICカード４００が接続され、ICカード４００が付属のICカードであるかを既に確認している。

再生装置２００は、入力部２１３から登録処理を開始する旨の入力を受け付けると（ス

テップＳ５１）、ID格納部２１１からID#2を読み出し（ステップＳ５２）、ID#2を含めて登録要求をAD内サーバ１００へ送信する（ステップＳ５３）。

【０１２９】

AD内サーバ１００を機器Aとし、再生装置２００を機器Bとして、前述の方法でSACを確立する（ステップＳ５４）。この際、AD内サーバ１００は、CSIとして「０」を使用し、再生装置２００は、CSI格納部２０８に格納しているCSIを使用する。

AD内サーバ１００は、ステップＳ３５の署名検証で、CSIとして「０」を用いて署名検証するので、検証結果が成功の場合は未登録であると判断し、失敗の場合は、登録済みであると判断する。再生装置２００が未登録であると判断する場合、登録情報を読み出し（ステップＳ５５）、残数が「０」か否かを判断する（ステップＳ５６）。「０」である場合（ステップＳ５６でYES）、登録不可通知を再生装置２００へ送信する（ステップＳ５７）。残数が「０」でない場合（ステップＳ５６でNO）、登録台数が「０」であるか否かを判断する（ステップＳ５８）。「０」である場合（ステップＳ５８でYES）、CSI生成部１０７でCSIを生成する（ステップＳ５９）。登録台数が「０」でない場合（ステップＳ５８でNO）、CSI格納部１０８からCSIを読み出す（ステップＳ６０）。生成又は読み出したCSIに、暗号化部１１９でセッション鍵SKを用いて暗号化アルゴリズムEを施して暗号化して暗号化CSIを生成し（ステップＳ６１）、暗号化CSIを再生装置２００へ送信する（ステップＳ６２）。

【０１３０】

再生装置２００は、登録不可通知を受信した場合、登録できないことをモニタ２５１に表示し（ステップＳ６３）、処理を終了する。暗号化CSIを受信した場合、復号部２１７で暗号化CSIを復号してCSIを生成し（ステップＳ６４）、CSI格納部２０８に格納する（ステップＳ６５）。また、AD内サーバ１００に受領通知を送信する（ステップＳ６６）。

再生装置２００から受領通知を受信すると、登録情報の機器IDに、ID#2を書き込み、登録台数に「１」を加算し、残数から「１」を減算する（ステップＳ６７）。

２．３　車載機器３００登録の動作

（１）AD内サーバ１００からICカード４００にCSIのコピーを許可する際の動作について、図１０を用いて説明する。

【０１３１】

ICカード４００がAD内サーバ１００に接続されると、ICカード４００は、ID格納部４１１からID#4を読み出し（ステップＳ７１）、AD内サーバ１００にID#4を送信する（ステップＳ７２）。

AD内サーバ１００は、ID#4を受信すると、登録情報からICカードIDを読み出し（ステップＳ７３）、受信したIDと読み出したIDとが一致するか否かを判断する（ステップＳ７４）。一致しない場合（ステップＳ７４でNO）、接続されたICカードが付属のICカードでないことを表示部１１４に表示し（ステップＳ７５）、処理を終了する。一致する場合（ステップＳ７４でYES）、処理を継続する。このように、接続されたICカードが付属のICカードであるか確認し、確認が済むと入力を受け付けるまで待機する。

【０１３２】

入力部１１３が、ICカード４００にCSIを記録する旨の入力を受け付けると（ステップＳ７６）、制御部１０１は、登録情報記憶部１０６から残数を読み出して（ステップＳ７７）、残数が「０」か否かを判断し（ステップＳ７８）、「０」である場合は（ステップＳ７８でYES）、登録出来ないことを表示部１１４に表示する（ステップＳ７９）。残数が「０」でない場合（ステップＳ７８でNO）、ICカード４００にCSIのコピーを１回許可する許可権利を送信する（ステップＳ８０）。

【０１３３】

ICカード４００は、AD内サーバ１００から許可権利を受信すると、コピー回数に「１」を加算し（ステップＳ８１）、AD内サーバ１００に受領通知を送信する（ステップＳ８２）。

AD内サーバ１００は、受領通知を受信すると、登録情報の登録台数に「１」を加算し、

残数から「１」を減算し（ステップＳ８３）、処理を終了する。
（２）ICカード４００から車載機器３００にCSIをコピーする際の動作について、図１１を用いて説明する。
【０１３４】
ICカード４００が車載機器３００に接続されると、ステップＳ７１～７５の処理を行い、ICカードIDを確信する。また、ICカード４００を機器Aとして、車載機器３００を機器BとしてSACの確立処理を行い、セッション鍵SKを共有する（ステップＳ９１）。この際、ICカード４００はCSIの初期値である「０」を用いて認証を行い、車載機器３００は、CSI格納部３０８に格納している値を用いて認証を行う。
【０１３５】
ICカード４００の制御部４０１は、ステップＳ３５の署名検証で、CSIとして「０」を用いて署名検証するので、検証結果が成功の場合は未登録であると判断し、失敗の場合は、登録済みであると判断する。登録済みと判断する場合（ステップＳ９２でNO）、車載機器３００へ登録不可通知を送信し（ステップＳ９３）、処理を終了する。未登録であると判断する場合（ステップＳ９２でYES）、ステップＳ１８で受け取る、車載機器３００のID#3をID記憶部４２０に記憶する（ステップＳ９４）。暗号化部４１８は、公開鍵暗号処理部４０５からセッション鍵SKを受け取ると、CSI格納部４０８からCSIを読み出す（ステップＳ９５）。セッション鍵SKを用いてCSIを暗号化して暗号化CSIを生成し（ステップＳ９６）、生成した暗号化CSIを入出力部４１６を介して車載機器３００へ送信する（ステップＳ９７）。
【０１３６】
車載機器３００の制御部３０１は、ICカード４００から登録不可通知を受け取った場合、登録済みであることをモニタ３２２に表示し（ステップＳ９８）、登録処理を終了する。ICカード４００から暗号化CSIを受信した場合、復号部３１７は公開鍵暗号処理部３０５からセッション鍵SKを受け取り、セッション鍵SKを用いて暗号化CSIを復号してCSIを生成し（ステップＳ９９）、生成したCSIをCSI格納部３０８へ格納する（ステップＳ１００）。また、受領通知をICカード４００へ送信する（ステップＳ１０１）。
【０１３７】
ICカード４００は、車載機器３００から受領通知を受信すると、コピー回数から「１」を減算し（ステップＳ１０２）、処理を終了する。
（３）CSIをコピーしたことをAD内サーバ１００に通知する際の動作
ICカード４００がAD内サーバ１００に接続されると、AD内サーバ１００は、ICカード４００のIDを確認して付属のICカードであるか確認し、確認が済むと入力を受け付けるまで待機する。
【０１３８】
ICカード４００は、ID記憶部４２０からコピー先のIDであるID#3を読み出し、ID#3を含むコピー通知をAD内サーバ１００へ送信する。
AD内サーバ１００は、コピー通知を受信すると、コピー通知に含まれるID#3を、登録情報に機器IDとして記憶する。また、ICカード４００へ、受領通知を送信し、処理を終了する。
【０１３９】
ICカード４００は、AD内サーバ１００から受領通知を受信すると、処理を終了する。
２．４　コンテンツ配送の動作１
AD内サーバ１００から再生装置２００へコンテンツを配信し、再生する際の動作を、図１２を用いて説明する。
再生装置２００は、入力部２１３からコンテンツを取得する旨の入力を受け付けると（ステップＳ１２１）、AD内サーバ１００へコンテンツの配送要求を送信する（ステップＳ１２２）。
【０１４０】
AD内サーバ１００及び再生装置２００は、SACを確立する（ステップＳ１２３）。この

際、それぞれCSI格納部に格納しているCSIを用いて認証を行う。
AD内サーバ１００は、ステップＳ３５の処理で、再生装置２００が同一AD内の機器であることを確認する。
認証が失敗の場合（ステップＳ１２４でNO）、AD内サーバ１００は、再生装置２００へ配送不可通知を送信し（ステップＳ１２５）、処理を終了する。認証が成功の場合（ステップＳ１２４でYES）、AD内サーバ１００は、コンテンツ鍵格納部１１８から暗号化コンテンツ鍵aを読み出し（ステップＳ１２６）、復号部１１７で復号し（ステップＳ１２７）、更に、暗号化部１１０にて、認証の際に共有したセッション鍵SKを用いて暗号化して暗号化コンテンツ鍵ｓを生成し（ステップＳ１２８）、生成した暗号化コンテンツ鍵ｓを再生装置２００へ送信する（ステップＳ１２９）。また、コンテンツ格納部１０９から暗号化コンテンツを読み出し（ステップＳ１３０）、再生装置２００へ送信する（ステップＳ１３１）。

【０１４１】
再生装置２００は、配送不可通知を受信した場合、モニタ２５１に配送できない旨を表示し（ステップＳ１３２）、処理を終了する。暗号化コンテンツ鍵ｓを受信した場合、セッション鍵SKを用いて復号部２１７にて復号してコンテンツ鍵を生成し（ステップＳ１３３）、生成したコンテンツ鍵を復号部２２０へ出力する。復号部２２０は、復号部２１７から受け取ったコンテンツ鍵を用いて、AD内サーバ１００から受け取る暗号化コンテンツに復号アルゴリズムDを施してコンテンツを生成し（ステップＳ１３４）、再生部２２１へ出力する。再生部２２１は、受け取ったコンテンツから映像信号及び音声信号を生成してモニタ２５１及びスピーカ２５２へ出力し、コンテンツを再生する（ステップＳ１３５）。

２．５　コンテンツ配送の動作２
AD内サーバ１００から受信したコンテンツを、再生装置２００内に一旦蓄積してから再生する際の動作を、図１３を用いて説明する。

【０１４２】
ステップＳ１２１からステップＳ１３０までは同様の処理を行う。
復号部２１７は、暗号化コンテンツ鍵ｓを復号してコンテンツ鍵を生成し（ステップＳ１４１）、生成したコンテンツ鍵を暗号化部２１８へ出力する。暗号化部２１８は、CSI格納部２０８からCSIを読み出し、ID格納部２１１からID#2を読み出す（ステップＳ１４２）。ID#2及びCSIをこの順で連結してID#2||CSIを生成し（ステップＳ１４３）暗号化鍵ｂとする。生成した暗号化鍵ｂを用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵ｂを生成し（ステップＳ１４４）、暗号化コンテンツ鍵ｂをコンテンツ鍵格納部２１９へ格納する（ステップＳ１４５）。また、AD内サーバ１００から暗号化コンテンツを受信すると、コンテンツ格納部２０９へ格納する（ステップＳ１４６）。

【０１４３】
入力部２１３から格納したコンテンツを再生する旨の入力を受け付けると（ステップＳ１４７）、復号部２１７は、コンテンツ鍵格納部２１９から暗号化コンテンツ鍵ｂを読み出す（ステップＳ１４８）。また、CSI格納部２０８からCSIを読み出し、ID格納部２１１からID#2を読み出し（ステップＳ１４９）、ID#2及びCSIを連結してID#2||CSIを生成し（ステップＳ１５０）、復号鍵とする。生成した復号鍵を用いて暗号化コンテンツ鍵ｂに復号アルゴリズムDを施してコンテンツ鍵を生成し（ステップＳ１５１）、生成したコンテンツ鍵を復号部２２０へ出力する。復号部２２０及び再生部２２１は、ステップＳ１３２～ステップＳ１３３の処理を行い、コンテンツを再生する。

２．６　DVDに記録する際の動作
AD内サーバ１００でDVD５００にコンテンツを書き込む際の動作を、図１４を用いて説明する。

【０１４４】
AD内サーバ１００は、入力部１１３からコンテンツをDVDに記録する旨の入力を受け付けると（ステップＳ１６１）、コンテンツ鍵格納部１１８から暗号化コンテンツ鍵ａを読

み出し（ステップＳ１６２）、ID格納部１１１からID#1を読み出し、CSI格納部１０８からCSIを読み出す（ステップＳ１６３）。復号部１１７は、ID#1とCSIとを連結して復号鍵を生成し（ステップＳ１６４）、生成した復号鍵を用いて暗号化コンテンツ鍵ａを復号してコンテンツ鍵を生成し（ステップＳ１６５）、生成したコンテンツ鍵を暗号化部１１０へ出力する。暗号化部１１０は、コンテンツ鍵を受け取ると、登録情報記憶部１０６から機器ＩＤを読み出し、CSI格納部１０８からCSIを読み出す（ステップＳ１６６）。読み出したID#2とCSIとを連結して暗号鍵ｂを生成し、ID#3とCSIとを連結して暗号鍵ｃを生成する（ステップＳ１６７）。生成した暗号鍵ｂ及び暗号鍵ｃをそれぞれ用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵ｂ及び暗号化コンテンツ鍵ｃを生成する（ステップＳ１６８）。生成した暗号化コンテンツ鍵ｂ及び暗号化コンテンツ鍵ｃをDVD５００に書き込む（ステップＳ１６９）。また、コンテンツ格納部１０９から暗号化コンテンツを読み出し（ステップＳ１７０）、DVD５００に書き込む（ステップＳ１７１）。

２．７　再生装置２００脱退の動作

AD内サーバ１００から再生装置２００が脱退する際の動作を図１５を用いて説明する。

【０１４５】

なお、AD内サーバ１００は、ICカード４００が接続され、既にICカードIDを確認している。

再生装置２００は、入力部２１３から脱退する旨の入力を受け付けると（ステップＳ１８１）、ID格納部２１１からID#2を読み出し（ステップＳ１８２）、ID#2を含めて脱退要求をAD内サーバ１００に送信する（ステップＳ１８３）。

【０１４６】

AD内サーバ１００及び再生装置２００は、認証を行い、SACを確立する（ステップＳ１８４）。この際、それぞれCSI格納部に格納しているCSIを用いて認証を行う。

AD内サーバ１００は、ステップＳ３５の処理で、再生装置２００がAD内の機器として登録しているか否かを判断し、未登録の場合（ステップＳ１８５でNO）、未登録通知を再生装置２００へ送信する（ステップＳ１８６）。登録済みの場合は（ステップＳ１８５でYES）、CSI削除通知を送信する（ステップＳ１８７）。

【０１４７】

再生装置２００は、未登録通知を受信すると、モニタ３２２に未登録であることを表示し（ステップＳ１８８）、処理を終了する。削除通知を受信すると、CSI格納部２０８からCSIを削除する（ステップＳ１８９）。また、削除完了通知をAD内サーバ１００へ送信する（ステップＳ１９０）。

AD内サーバ１００は、削除完了通知を受信すると、機器IDからID#2を削除し、登録台数から「１」を減算し、残数に「１」を加算する（ステップＳ１９１）。

３．　その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）本実施の形態で、AD内サーバ１００と接続されていない機器を登録する際に、ICカード４００を用いてCSIをコピーするとしたが、クライアント機器間でCSIを移動するとしても良い。

【０１４８】

再生装置２００から再生装置２００ｎにCSIを移動し、再生装置２００ｎをAD内機器として登録する際を例として説明する。

再生装置２００と再生装置２００ｎとを接続し、再生装置2.００ｎを操作して移動通知を再生装置２００に送信する。再生装置２００及び再生装置２００ｎは、SACを確立してセッション鍵SKを生成する。再生装置２００は、セッション鍵SKでCSIを暗号化して再生装置２００ｎへ送信する。再生装置２００ｎは、セッション鍵を用いて暗号化CSIを復号して格納し、SAC確立の際に受け取った移動元である再生装置２００のIDを記憶する。また、再生装置２００へ受領通知を送信する。再生装置２００は、受領通知を受信すると、CSI格納部２０８のCSIを削除して、「０」を格納する。

【０１４９】
再生装置２００ｎは、AD内サーバ１００に接続され、SACを確立すると、AD内サーバ１００にCSIを移動されたことを通知し、移動元のID及び再生装置２００ｎのIDを送信し、AD内サーバ１００は、登録情報の機器IDを書き換える。
（２）ICカード４００はAD内サーバ１００に付属の機器であるとしたが、付属でなくても良い。
【０１５０】
ICカード４００も他のクライアント機器と同様に、AD内サーバ１００に接続されるとSACを確立し、ID#４を機器IDとして登録し、CSIを取得する。
AD内サーバ１００は、DVD５００にコンテンツ鍵を記録する際、コンテンツ鍵をICカード４００のID#4とCSIとを連結して生成した暗号鍵を用いて暗号化する。
車載機器３００は、DVD５００が装着され、ICカード４００が接続されると、ICカード４００との間でSACを確立してセッション鍵を共有する。
【０１５１】
ICカード４００は、ICカード４００内に記憶しているID#4とCSIとを連結して復号鍵を生成し、セッション鍵SKを用いて復号鍵を暗号化して暗号化復号鍵を生成して車載機器３００へ送信する。
車載機器３００は、暗号化復号鍵をセッション鍵SKを用いて復号して復号鍵を生成し、DVDから読み出す暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、コンテンツ鍵を用いて暗号化コンテンツを復号してコンテンツを再生する。
【０１５２】
また、上記（１）のように、クライアント間でCSIを移動する場合と同様の処理を行い、ICカードから車載機器３００にCSIを移動しても良い。この場合、実施の形態１のICカード４００と同様に、付属でないICカードに、AD内サーバ１００へ移動を通知する機能を持たせても良い。車載機器３００にCSIを移動したICカードは、その場でCSIを削除せずに、CSIの移動を禁止し、AD内サーバ１００に移動を通知した後にCSIを削除する。
（３）ICカード４００を用いてAD内サーバ１００に接続されていない機器を登録する場合、ネットワークを介してAD内サーバ１００からICカード４００に許可権利又はCSIを送信するとしても良い。
【０１５３】
一例として、PCなどネットワークに接続して通信する機能を有するクライアント機器に、ICカード４００が接続されると、ICカード４００は、PCの通信機能を利用して、SAC確立の処理を行い、許可権利又はCSIを受信する。
通信機能を有するクライアント機器は、PCに限らず、PDAや携帯電話などであっても良い。
（４）本実施の形態では、AD内サーバ１００からクライアント機器へコンテンツを配送、又はDVDに記録して配布するとしたが、クライアント機器間でSACを確立してセッション鍵SKを生成し、コンテンツを配送するとしても良い。
（５）本実施の形態で、ICカード４００を用いて車載機器３００を登録するとしたが、同様にICカード４００を用いて、脱退の処理を行っても良い。
【０１５４】
この場合、ICカード４００を接続された車載機器３００を操作して、ICカード４００へ脱退要求を送信し、ICカード４００は、SACを確立して車載機器３００が登録済みであることを確認し、車載機器３００へ削除通知を送信する。車載機器３００は、CSIを削除し、ICカード４００へ削除完了通知を送信する。ICカード４００は、削除完了通知を受信すると、脱退した車載機器３００のIDを記憶する。ICカード４００は、AD内サーバ１００に接続されると、AD内サーバ１００に、車載機器３００が脱退した旨と、車載機器３００のIDとを通知する。AD内サーバ１００は、機器IDから車載機器３００のIDを削除し、登録台数から「１」減算し、残数に「１」を加算する。
（６）本実施の形態でAD内サーバ１００は、SACを確立する際の署名検証で相手機器が格

納しているCSIの値によって、相手機器が未登録であるか登録済みであるかを確認するとしたが、認証する機器からIDを受信し、登録情報の機器IDに、受信したIDが記憶されているか否かによって、未登録か、登録済みかを確認するとしても良い。また、AD内の機器として登録されているクライアント機器全てが、登録されているIDを記憶しておき、クライアント機器間でも同様に、IDによって、登録、未登録を確認するとしても良い。

（７）AD内サーバ１００と接続されていない機器を登録する際、ICカード４００を用いるとしたが、AD内サーバ１００がCSIを表示部１１４に表示し、それをユーザがクライアント機器に手入力するとしても良い。この場合、入力するコードは、機器やセッションに依存してCSIを暗号化した値であっても良い。

（８）本実施の形態で、SACを確立し、CSIを暗号化して送信する際、暗号文に暗号化CSIを送信する機器の署名データを付加して送信するとしても良い。

（９）本実施の形態で、登録情報及びCSIは、それぞれの機器の内部に格納されるとしたが、着脱可能で、許可なく読み出し、書き込み及びコピーが出来ない領域に格納するとしても良い。

（１０）本実施の形態で、コンテンツを暗号化する際の暗号化鍵、又は復号する際の復号鍵として、機器のID及びCSI又は乱数及びCSIを連結して利用するとしたが、この限りではなく、機器のID及びCSI又は乱数及びCSIを用いて演算を行い、その結果得られる値を用いるとしても良い。

（１１）本実施の形態では、登録情報として、最大数、登録台数及び残数を管理するとしたが、これに限らない。

【０１５５】

最大数を残数の初期値とし、登録する度に残数から「１」ずつ減らし、残数が「０」でなければクライアント機器を登録するとしてもよい。また、最大数と、登録台数とを管理し、登録台数が最大数以下であれば、クライアント機器を登録するとしても良い。

（１２）登録情報の機器の台数は、AD内サーバ１００とオンラインで接続している機器と、ICカード４００を用いて登録する機器とを分けて、最大数、登録台数などを管理しても良い。

（１３）本実施の形態では、AD内サーバ１００が記憶している登録情報を基に管理しているが、別途管理機関を設け、以下（ａ）～（ｃ）のようにしても良い。

【０１５６】

（ａ）管理機関が最大数を設定し、最大数に管理機関の署名データを付して、DVDなどの可搬型の記録媒体に記録して配布、又は通信を介して配布する。AD内サーバ１００は、署名データを検証し、検証結果が成功の場合に、最大数として記憶する。

（ｂ）AD内サーバ１００は、登録したい台数を管理機関に要求する。管理機関は、台数に応じた課金を行い、課金に成功した場合に、要求した台数の登録を許可する情報をAD内サーバ１００へ送信し、AD内サーバ１００は情報を受け取ると、許可された台数の範囲内でクライアント機器の登録を受け付ける。

【０１５７】

（ｃ）AD内サーバ１００は、クライアント機器からの登録を受け付ける度に、管理機関に要求を出し、管理機関は、要求に対して課金を行い、課金に成功すると、登録を許可する。AD内サーバ１００は、許可されると、クライアント機器を登録し、CSIを送信する。

（１４）再生装置２００は、AD内サーバ１００から配送されたコンテンツを再生するとしたが、DVD再生機能を有し、AD内サーバ１００によってDVD５００に記録されたコンテンツを再生するとしても良い。

【０１５８】

また、AD内サーバ１００は、登録情報に記憶している機器ID全てを、それぞれCSIと連結してコンテンツ鍵の暗号化に用いるとしたが、DVDを再生する機能を有する機器のIDを予め記憶しておき、DVDを再生できる機器のIDを抽出し、それぞれCSIと連結してコンテンツ鍵の暗号化に用いるとしても良い。

（１５）本実施の形態では、AD内サーバ１００はDVDにコンテンツを記録するとしたが、

メモリーカード、MD、MO、CD、BD（Blu-ray Disk）などに記録するとしても良いし、ICカードにコンテンツを記録するとしても良い。

【０１５９】

また、クライアント機器は、再生装置の他、記録装置でもよく、それらを組み合わせたものであってもよい。また、クライアント機器は、ユーザ宅内に設置されている又は車両に搭載されている他、ユーザが持ち運ぶことができる携帯型の機器であっても良い。

（１６）ICカード４００は、AD内サーバ１００又は車載機器３００に直接接続されるため、SACの確立処理を行わなくても良い。

（１７）SAC確立の際、乱数Cha#B又はCha#Aに、CSIを連結したデータに対して署名データ生成するとしたが、署名対象と成るデータのハッシュ値を計算し、このハッシュ値に対して署名データを生成するとしても良い。

（１８）SAC確立の際、認証相手の機器が未登録か登録済みかを判断するとき及び鍵共有のときにCSI利用するとしたが、どちらか一方に利用するとしても良い。

【０１６０】

また、本実施の形態では双方向に認証を行っているが、片方向認証であっても良い。

（１９）クライアント機器の登録を、時間で制限するとしても良い。

AD内サーバ１００とクライアント機器との間で時間を合わせる。AD内サーバ１００は、CSIの使用を許可する期間を設定して有効期限情報とし、有効期限情報とCSIとをクライアント機器に送信し、登録台数から「１」減算する。

【０１６１】

クライアント機器は、有効期限情報及びCSIを受信し、格納する。有効期限情報が示す期間が終了すると、CSIを削除する。

AD内サーバ１００は、有効期限情報が示す期間が終了すると、登録台数に「１」を加算する。機器IDを記憶している場合は、期限が切れた機器のIDを削除する。

なお、有効期限情報は、有効期限の開始と終了の日時を示す情報でも良いし、終了の日時のみ示すものであっても良い。また、CSIの使用開始からの期間を制限するものであっても良いし、CSIを使用してクライアント機器が動作している期間を制限するとしても良い。

（２０）本実施の形態では、AD内サーバは１つであるとして説明したが、一つのＡＤに複数のAD内サーバがあっても良い。

【０１６２】

この場合、クライアント機器は、何れのAD内サーバと通信するかを選択することが出来る。選択方法として、ユーザが設定するとしても良いし、クライアント機器がAD内で、当該クライアントと距離が最短のAD内サーバを選択しても良い。また、AD内サーバのうち、処理能力が高いものや、他のタスクが少ないAD内サーバを選択するとしても良い。

また、以下のように、クライアント機器から登録を要求されたAD内サーバが、それ以上クライアント機器を登録出来ない場合、登録可能な他のAD内サーバを探すとしても良い。

【０１６３】

クライアント機器は、１つのAD内サーバに登録要求を送信する。登録要求を受信したAD内サーバは、登録台数が最大数と一致する場合、他のAD内サーバに、クライアント機器を登録できるか問い合わせる。他のAD内サーバは、登録可能である場合、要求元のクライアント機器を登録し、AD内サーバに登録可能である旨を応答し、AD内サーバは、クライアント機器へCSIを送信する。

【０１６４】

また、他のAD内サーバが登録できない旨を応答した場合、AD内サーバは、更に他のAD内サーバへ問い合わせる。

また、複数のAD内サーバ間で代表となるAD内サーバを決定し、代表サーバが全てのグループ内機器を管理するとしても良い。この場合、代表で無いAD内サーバがクライアント機器から登録要求を受け付けると、代表サーバに登録可能であるか問い合わせ、登録可能で有る場合、クライアント機器は代表サーバに登録され、代表サーバから要求を受け付けた

AD内サーバを介してCSIを受け取る。

【０１６５】

なお、要求を受け付けたAD内サーバが、他の処理を行っている場合などに、他のAD内サーバへ問い合わせるとしても良い。

また、以下（ａ）、（ｂ）のように、複数のAD内サーバ間で、登録した機器の台数を管理するために、登録した機器に関するリストを共有するとしても良い。

（ａ）同一ＡＤ内のAD内サーバＲ及びAD内サーバＳはそれぞれ、クライアント機器を登録すると、登録した機器のＩＤを機器リストとして記憶する。また、ＩＤを書き込むことでリストが更新される度に、バージョン番号を機器リストに対応付けて記憶する。

【０１６６】

AD内サーバＲ及びＳは、定期的又は不定期に前記機器リストを交換する。AD内サーバＲは、自分が記憶している機器リストのバージョン番号と、AD内サーバＳから受け取った機器リストのバージョン番号とを比較し、より新しい方を機器リストとして記憶する。AD内サーバＳも同様に処理する。これにより、常に最新の機器リストを共有することが出来る。

【０１６７】

なお、一方のAD内サーバの機器リストが更新されるたびに機器リストを交換するとしても良い。また、機器リストだけでなく、登録台数、最大数など、登録情報も、上記と同様に共有するとしても良い。

（ｂ）同一ＡＤ内のAD内サーバT及びAD内サーバUはそれぞれ機器リストT及び機器リストUを保持しており、それぞれクライアント機器を登録する際、機器ＩＤと登録した時刻とを対応付けて格納する。AD内サーバT及びAD内サーバUは、定期的又は不定期に機器リストを交換する。

【０１６８】

AD内サーバTは、自分が登録情報として記憶している登録台数が最大数より少なければ、AD内サーバUから受け取った機器リストUに、新しく登録されたクライアント機器を、登録された順に、自分が保持している機器リストTに書き込む。また、AD内サーバUも同様に、機器リストTを受け取り、新しく登録された順に機器リストUを更新する。

なお、予めクライアント機器に優先順位を付しておき、優先順位が高い機器を優先的に登録するとしても良い。また、AD内サーバT及びUに新しく登録されたクライアント機器を合わせると最大数を超える場合、優先順位の高い機器を優先的に登録するとしても良いし、ユーザが登録する機器を選択しても良い。

【０１６９】

この方法によると、一方のAD内サーバが電源を切っていても、他方のAD内サーバに登録でき、他方のAD内サーバが更新されると、機器リストを交換して整合性を保つので、AD内サーバ間で同一の機器リストを共有することが出来る。

（２１）各ADのCSIの重複を回避するために、それぞれのADを管理するAD内サーバ間で情報を交換して、重複しているか否かを確認するとしても良い。

【０１７０】

また、安全性を高めるために、AD内サーバは、それぞれのCSIをハッシュ関数に入力してハッシュ値を算出し、ハッシュ値を交換して重複しているか確認するとしても良い。

また、AD内サーバがCSIを生成する代わりに、管理機関を設けて、管理機関が全てのADのCSIを重複しないように生成し、各AD内サーバに安全に送付するとしても良い。

（２２）クライアント機器は複数のADに属するようにしてもよい。

【０１７１】

また、クライアント機器が、格納できるCSIの数を制限することで、登録出来るADの数を制限するとしても良い。また、各AD内サーバが登録されているクライアント機器のリスト情報を交換して、１つのクライアント機器が登録できるADの個数を制限する構成であっても良い。また、リスト情報の交換により、クライアント機器がいくつのADに属しているかを確認することが出来る。

【０１７２】
別途、クライアント機器が登録しているADの数を管理する管理機関を設けても良い。
また、１台のAD内サーバは、複数のADを管理するとしても良い。この場合、AD内サーバは、それぞれ異なるCSIを格納できる数を制限されており、この数以内のADを管理できる。また、AD内サーバは、登録可能なクライアント機器の台数をCSI毎に記憶していても良いし、ＣＳＩとグループのＩＤとを対応付けて記憶するとしても良い。
（２３）ADは、それぞれ識別子を割り当てられており、コンテンツを配送する際に、コンテンツの配送元の機器は、当該機器が登録しているADの識別子を電子透かしとしてコンテンツに埋め込むとしても良い。
【０１７３】
これにより、クライアント機器が復号したコンテンツを、不正にAD外に配布した場合に、そのコンテンツがどのADから流出したのかを特定することが出来る。更に、コンテンツの配信元のサーバが、各ADに登録しているクライアント機器のIDを管理している場合、コンテンツを流出したクライアント機器のIDをCRLに載せても良い。
（２４）本実施の形態では、機器の認証後にコンテンツを配送するとしたが、本発明はこれに限定されない。
【０１７４】
コンテンツを配送する際、以下のように、認証を行わないとしても良い。
コンテンツの送信側の機器は、CSIを基にして暗号鍵を生成する。生成した暗号鍵を用いてコンテンツ鍵を暗号化し、暗号化コンテンツと暗号化コンテンツ鍵とを配送する。
受信側の機器は、暗号化コンテンツと暗号化コンテンツ鍵とを取得すると、CSIを基にして、暗号鍵と同一の復号鍵を生成する。生成した復号鍵を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、コンテンツ鍵を用いて暗号化コンテンツを復号してコンテンツを生成する。
【０１７５】
これによると、CSIを保持する機器のみが復号鍵を生成し、コンテンツを復号することが出来る。
また、認証せずに、暗号化コンテンツのみ配送し、その後、実施の形態と同様に認証を行ってセッション鍵を共有し、認証に成功した場合に、セッション鍵でコンテンツ鍵を暗号化して配送するとしても良い。
【０１７６】
なお、暗号化コンテンツの配送は、通信で配送するとしても良いし、可搬型の記録媒体に記録して配布するとしても良い。
また、受信側の機器からの要求に応じてコンテンツを配送する他、要求がなくても送信側の機器が判断して配送するとしても良いし、外部からの入力に従って、配送するとしても良い。
（２５）本実施の形態で、CSI格納部は、初期値として「０」を記憶しており、AD内サーバ１００が生成したCSIを取得すると、取得したCSIを上書きするとしたが、初期値とCSIとを別の領域に記憶しても良い。また、取得したCSIを初期値とは別の領域に記憶すると、初期値の使用を抑制するとしても良い。
【０１７７】
なお、使用を抑制した初期値は、移動、脱退などでCSIを削除した際に、再度活性化される。
なお、未登録を示す値として「０」を格納するとしたが、「０」でなくても良く、CSIとして生成される値と異なる値であればよい。
（２６）本実施の形態でAD内サーバ１００はICカード４００にCSIのコピーを１回許可しているが、複数回の許可を与えても良い。
【０１７８】
また、ICカード４００は、CSIを用いてクライアント機器を認証する他、CSIをコピーしたクライアント機器のIDを記憶しておき、コピーする際にクライアント機器のIDを確認す

ることで、同じクライアント機器へ複数回CSIをコピーすること防ぐとしても良い。
また、クライアント機器の登録処理を行う機能をICカードに実装し、ICカードを接続された機器がAD内サーバとして動作するとしても良い。

【０１７９】
また、クライアント機器が複数のクライアント機器の代表としてAD内サーバに登録し、他の複数のクライアント機器にCSIをコピーする権利を受けるとしても良い。以下に、図１６を用いて一例を示す。
ユーザ宅にはAD内サーバ６００と、クライアント機器６０１とが設置されており、クライアント機器６０１は既にAD内サーバ６００に登録されている。AD内サーバ６００は、登録情報として最大と残数とを記憶しており、ここでは最大が４、残数が３であるとする。

【０１８０】
ユーザが所有する車両には、AD内サーバ６００に登録されていない車載機器６０２，６０３，６０４が搭載されている。車載機器６０３，６０４は、AD内サーバ６００と直接通信する機能を持たない。車載機器６０２は、可搬型でAD内サーバ６００と直接通信する機能を有する。また、車載機器６０２～６０４は、それぞれ接続して通信可能である。
車載機器６０２は、車載機器の代表として、AD内サーバ６００に接続されると、登録したいクライアント機器の台数である希望台数３を含む登録要求をAD内サーバ６００へ送信する。

【０１８１】
AD内サーバ６００は、登録要求を受信すると、実施の形態と同様に車載機器６０２を認証し、セッション鍵を共有する。認証に成功した場合、登録要求に含む希望台数が、登録情報として記憶している残数以下であるかを判断する。残数以下であると判断する場合、記憶しているCSIを読み出し、読み出したCSIと、３台分の登録を許可する許可権利とを、セッション鍵を用いて暗号化し、暗号化権利情報として車載機器６０２に送信する。

【０１８２】
車載機器６０２は、暗号化権利情報を受信すると、セッション鍵を用いて復号し、CSI及び許可権利を生成する。また、生成したCSIを記憶することで、許可権利の内、１台分の許可権利を使ったので、残り２台登録できることを示す許可権利を記憶する。また、車載機器６０３及び６０４と、それぞれ認証を行い、成功するとCSIを送信し、送信した台数分の許可権利を減らす。

【０１８３】
これによって、車載機器６０２～６０４をクライアント機器として登録できる。
なお、残数が希望台数未満である場合、残数が示す台数分だけ登録を許可する許可権利を送信する。例として、２台分の許可権利を送信した場合、車載機器６０２は、CSIを記憶することで１台分の許可権利を使い、車載機器６０３，６０４の何れかにCSIを送信することでもう１台分の許可権利を使う。CSIの送信先の機器は、ユーザが選択するとしても良いし、それぞれの機器が予め優先順位を有し、優先順位の高い機器に送信するとしても良い。

【０１８４】
また、車載機器６０２～６０４をAD内サーバ６００に登録する際、各車載機器のIDをAD内サーバ６００に登録する場合、以下のように処理する。
車載機器６０２は、登録する前に、車載機器６０３及び６０４のIDを取得する。AD内サーバ６００に登録する際、取得したIDと、車載機器６０２自身のIDとをAD内サーバ６００に送信する。AD内サーバ６００は、受信したIDを機器IDとして記憶する。また、残数が希望台数未満である場合、AD内サーバ６００は、受け取ったIDの内、残数が示す台数分のIDを記憶する。この場合、登録するIDをユーザが選択するとしても良いし、予めIDに優先順位を付し、優先順位の高いIDから順に残数が示す台数分のIDを記憶するとしても良い。

【０１８５】
また、車載機器６０２は、許可権利が余ると、AD内サーバ６００に返すことが出来る。
なお、車載機器６０２は、当該車載機器６０２の権利を含めた許可権利を取得するとし

たが、車載機器６０２は、実施の形態と同様にAD内サーバ６００に登録し、車載機器６０３及び６０４にＣＳＩをコピーする権利を取得するとしても良い。
（２７）複数のADを合わせて１つのADを形成しても良い。
【０１８６】
一例として、AD#EとAD#Fとを合わせて、AD#Gを形成する場合を図１７、を用いて説明する。
AD#E及びAD#Fは、それぞれ１台のAD内サーバと、図示していない複数のクライアント機器とから構成される。AD#EのAD内サーバEは、最大ｍ台のクライアント機器が登録可能であり、AD#E内の機器は、それぞれCSI#Eを保持している。また、AD#FのAD内サーバFは、最大ｎ台のクライアント機器が登録可能であり、AD#F内の機器は、それぞれCSI#Fを保持している。
【０１８７】
この２つのADからAD#Gを形成する。まず、AD内サーバEとAD内サーバFとの間で、AD#Gを管理するAD内サーバGとなる機器を決定する。この際、処理性能、各AD内サーバの優先順位などを基に決定しても良いし、ユーザが決定しても良い。AD内サーバGでない方のAD内サーバは、クライアント機器としてAD#Gに登録される。
AD内サーバGに登録可能な台数ｋは、ｍ、ｎ又はｍとｎとの平均とする。また、AD内サーバGは、新たにCSI#Gを生成して、各クライアント機器を認証し、認証に成功した機器へCSI#Gを送信する。
【０１８８】
AD#EとAD#Fとを形成する機器の合計が、台数ｋを超える場合、登録する機器が選択される。この場合、予め設定されている優先順位を下にAD内サーバGが選択しても良いし、ユーザが選択するとしても良い。
なお、上述のように、２つのADから新たに１つのADを形成するほか、一方のADに他方のADを足しても良い。AD#EにAD#Fを足す場合、AD#F内の機器はAD#Eのクライアント機器としてAD内サーバEに登録され、CSI#Eを保持する。この際、登録するクライアント機器の台数が最大ｍ台を超える場合、上述のように、登録する機器が選択される。
【０１８９】
なお、ｍ、ｎ及びｋは、正の整数である。
（２８）１つのADから複数のADに分割するとしても良い。
一例として、AD#HからAD#IとAD#Jを形成する場合を、図１８を用いて説明する。
AD#Hは、AD#H内の機器を管理するAD内サーバHと、図示していない複数のクライアント機器とから構成される。
【０１９０】
AD内サーバHは、ｐ台（ｐは正の整数）のクライアント機器が登録可能であり、AD#H内の各機器はCSI#Hを格納している。
AD内サーバHは、AD#I及びAD#Jを形成する際、AD#H内のクライアント機器から新たにAD内サーバI及びAD内サーバJとなる機器を選択する。この際、処理能力が高い機器をAD内サーバとしても良いし、予め各機器に付されている優先順位を基に選択しても良い。また、ユーザが選択しても良いし、クライアント機器間で処理能力、優先順位などを基に選択しても良い。なお、AD内サーバHがAD内サーバI又はAD内サーバJとして、新たなADを形成するとしても良い。
【０１９１】
分割後、それぞれに属するクライアント機器が選択される。この際、優先順位を基にそれぞれのAD内サーバが選択しても良いし、ユーザが選択しても良い。AD内サーバI及びJは、それぞれ最大ｐ台のクライアント機器を登録可能である。また、各ADのクライアント機器を選択すると、AD内サーバIは、CSI#Iを生成し、選択されたクライアント機器へ、生成したCSI#Iを送信する。また、AD内サーバJも同様に、CSI#Jを生成してクライアント機器へ送信する。
【０１９２】

なお、AD内サーバI及びJは、クライアント機器を選択する度に認証しても良いし、新たに生成したCSIを送信する際に認証するとしても良い。

また、上記のように、１つのADから新たに２つのADを形成する他、AD#Hから新たなADを一つ形成し、基になったAD#Hと新たなADとの２つに分割するとしても良い。

（２９）クライアント機器が電源を切ると、クライアント機器はAD内サーバに登録されたまま、CSIは一旦削除されるとしても良い。

【０１９３】

この場合、クライアント機器がAD内サーバに登録されると、AD内サーバはクライアント機器のIDを記憶し、CSIを送信する。

クライアント機器は、受け取ったCSIを記憶すると、AD内機器としてコンテンツを利用できる。クライアント機器は、電源ＯＦＦの指示を受け付けると、CSIを削除し、電源をＯＦＦにする。この際、AD内サーバが記憶しているクライアント機器のIDは削除されない。

【０１９４】

再びクライアント機器の電源がＯＮになると、クライアント機器は、AD内サーバにIDを送信する。AD内サーバは、記憶しているIDに、受信したIDと一致するIDが有るか否かを判断し、一致するIDが有る場合、登録情報を更新せずに、クライアント機器にCSIを再送信する。

なお、有線又は無線通信が遮断された場合も同様にCSIを一旦消去し、通信が再度確立されると、ＩＤを送信し、CSIを再度取得するとしても良い。

（３０）本実施の形態では、CSIを用いて認証を行うとしたが、更に、以下の（ａ）～（ｃ）の認証を追加しても良い。

【０１９５】

（ａ）MACアドレスやIPアドレス、またシステムで統一的に与えられたコードなどを用いてクライアント機器がAD内サーバと同一の家庭内LANに接続されていることを認証する。これにより、他人のクライアント機器を登録することが困難になる。

また、AD内サーバとクライアント機器とが無線で通信を行う場合、電波の届く範囲であることで認証しても良い。

【０１９６】

また、AD内サーバとクライアント機器とが通信可能な場合、AD内サーバからクライアント機器へ、認証用データを送信し、クライアント機器は、認証用データを受信すると、応答データをAD内サーバへ送信する。AD内サーバは、認証用データを送信してから応答データを受信するまでの時間を計時し、計時した時間が、予め設定している閾値以内であれば、同一宅内に設置されているものと認証するとしても良い。

【０１９７】

また、TTL（Time To Live）値を宅内のルータの数以内に設定し、宅外の機器とは通信できないようにしても良い。

また、同じ電源に接続されているか否かを判断することで、同一宅内に設置されているか否かを認証するとしても良い。

（ｂ）AD内サーバに予めパスワードを設定しておき、クライアント機器を登録する際、ユーザは前記パスワードをクライアント機器に手入力する。クライアント機器は入力されたパスワードを含む登録要求をAD内サーバへ送信し、AD内サーバは、登録要求に含んで受信したパスワードが、予め設定されたパスワードと一致するか否かを判断する。

【０１９８】

また、パスワードは複数設定しても良く、例えば家族それぞれが自分のパスワードを設定するとしても良い。また、ユーザそれぞれを識別するＩＤとパスワードとを組み合わせるとしても良い。

（ｃ）上記（ｂ）におけるパスワードの代わりに、指紋や虹彩などのバイオメトリックス情報を使用しても良い。これにより、予め設定した本人だけがクライアント機器の登録を行うことが可能となる。

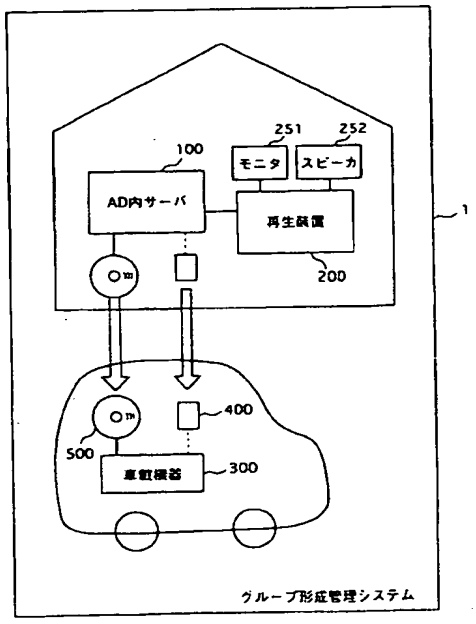
（３１）クライアント機器が保持している初期値は、以下（ａ）～（ｃ）の場合がある。
【０１９９】
（ａ）クライアント機器は、AD内サーバに登録していないことを示す、１個の初期値を保持している。当該AD内サーバに登録されると、初期値の使用が抑制される。
（ｂ）クライアント機器は、複数のAD内サーバそれぞれに対応する複数の初期値を保持している。複数のAD内サーバの何れかに登録する際、当該AD内サーバに対応する初期値を用いて認証し、登録されると、前記対応する初期値の使用を抑制する。また、他のAD内サーバに登録されると、他のAD内サーバに対応する初期値の使用を抑制する。
【０２００】
なお、それぞれの初期値をグループの識別子に対応付けて識別しても良い。
（ｃ）クライアント機器は、複数のAD内サーバの、何れにも登録していないことを示す初期値を保持している。何れかのAD内サーバに登録すると、初期値の使用を抑制する。
（３２）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。
【０２０１】
また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている
前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。
【０２０２】
また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。
また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。
【０２０３】
また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。
（３３）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。
【産業上の利用可能性】
【０２０４】
ディジタル著作物の不正利用を防止し、ユーザは自由にディジタルコンテンツを利用可能なグループの形成に利用できる。
【図面の簡単な説明】
【０２０５】
【図１】グループ形成管理システム１の全体の構成を示すブロック図である。
【図２】AD内サーバ１００の構成を示すブロック図である。
【図３】登録情報の構成を示す図である。
【図４】再生装置２００の構成を示すブロック図である。
【図５】車載機器３００の構成を示すブロック図である。
【図６】ICカード４００の構成を示すブロック図である。
【図７】SAC確立の処理を示すフローチャートである。図８に続く。
【図８】SAC確立の処理を示すフローチャートである。図７の続き。
【図９】再生装置２００をAD内サーバ１００に登録する際の動作を示すフローチャートである。

【図１０】車載機器３００を登録する際の動作を示すフローチャートである。
【図１１】車載機器３００を登録する際の動作を示すフローチャートである。
【図１２】コンテンツを配送する際の動作を示すフローチャートである。
【図１３】コンテンツを配送する際の動作の一部を示すフローチャートである。
【図１４】コンテンツをDVDに記録する際の動作を示すフローチャートである。
【図１５】AD内サーバ１００から脱退する際の動作を示すフローチャートである。
【図１６】複数のクライアント機器を、代表の機器がAD内サーバに登録する場合の構成を示すブロック図である。
【図１７】複数のグループから一つのグループを形成する場合の概念を示す図である。
【図１８】一つのグループを分割して複数のグループを形成する場合の概念を示す図である。

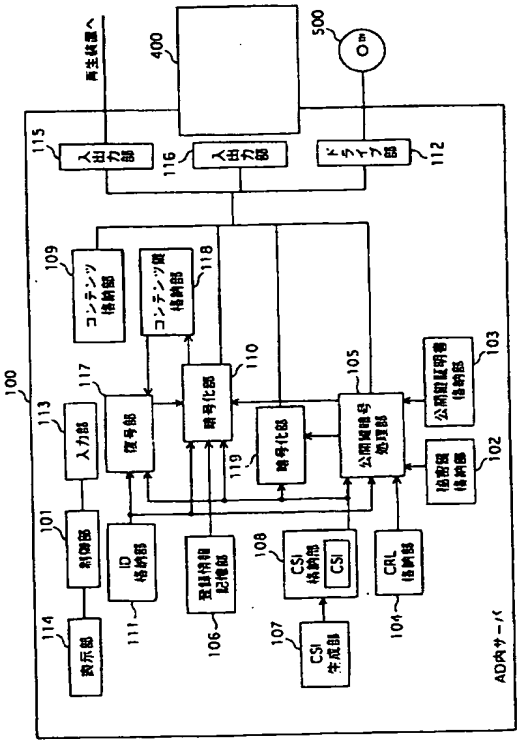
【符号の説明】
【０２０６】

| | |
|---|---|
| １ | グループ形成管理システム |
| １００ | ＡＤ内サーバ |
| ２００ | 再生装置 |
| ３００ | 車載機器 |
| ４００ | ＩＣカード |
| ５００ | ＤＶＤ |
| ６００ | AD内サーバ |
| ６０１ | クライアント機器 |
| ６０２，６０３，６０４ | 車載機器 |

【図１】




【図２】



【図３】

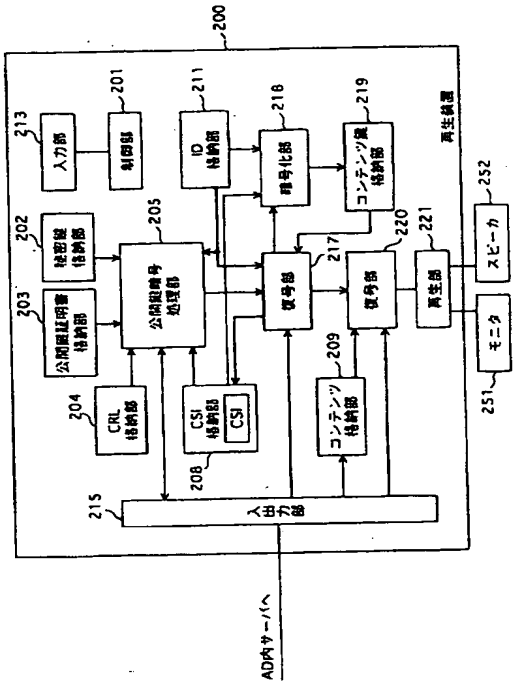
(a)

| 登録情報 | |
|---|---|
| 機器ID | |
| | |
| 最大 | 2 |
| 登録台数 | 0 |
| 残数 | 2 |
| ICカードID | ID_4 |

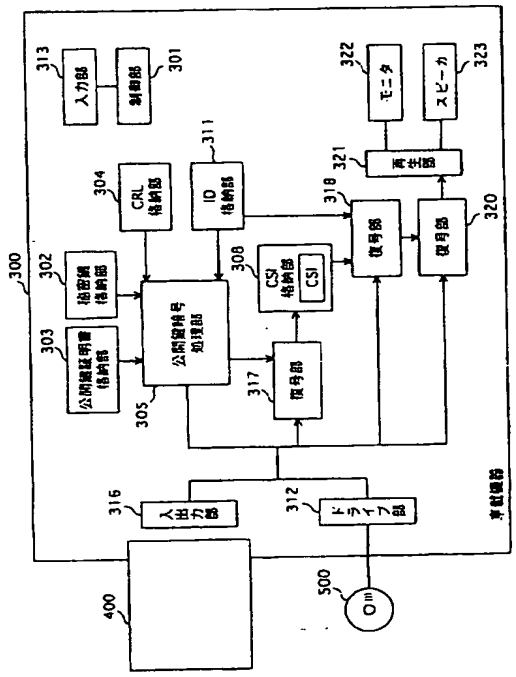
(b)

| 登録情報 | |
|---|---|
| 機器ID | ID_2 |
| | ID_3 |
| 最大 | 2 |
| 登録台数 | 2 |
| 残数 | 0 |
| ICカードID | ID_4 |

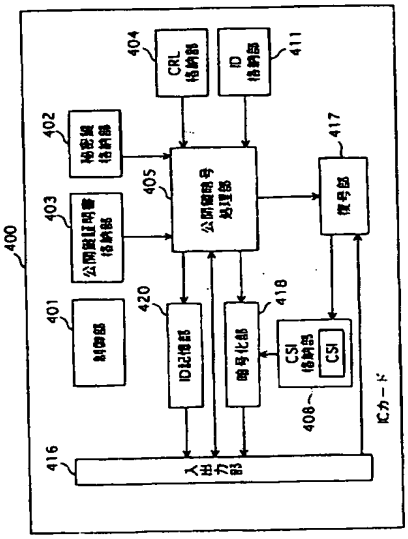
【図４】



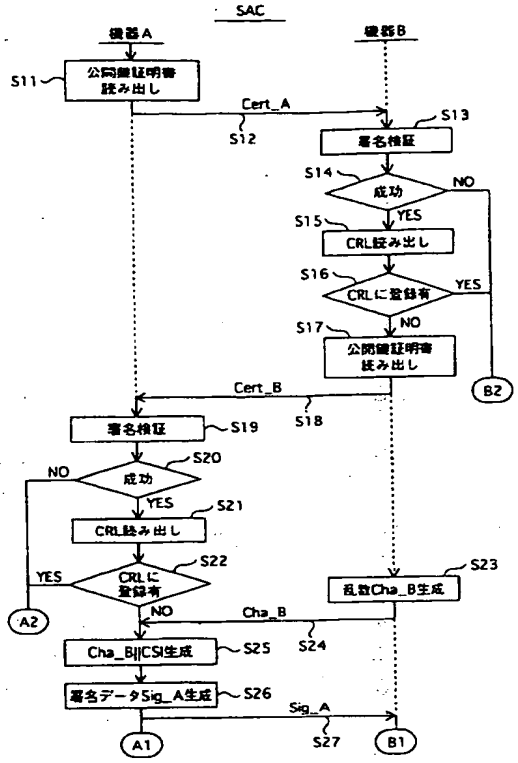

【図５】



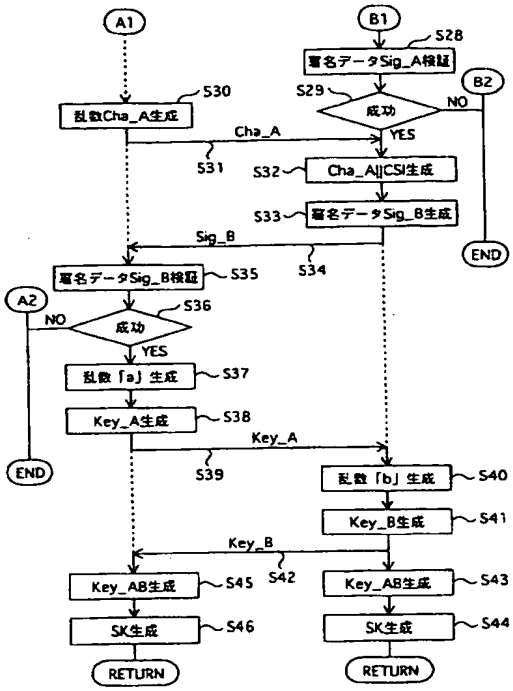

【図６】



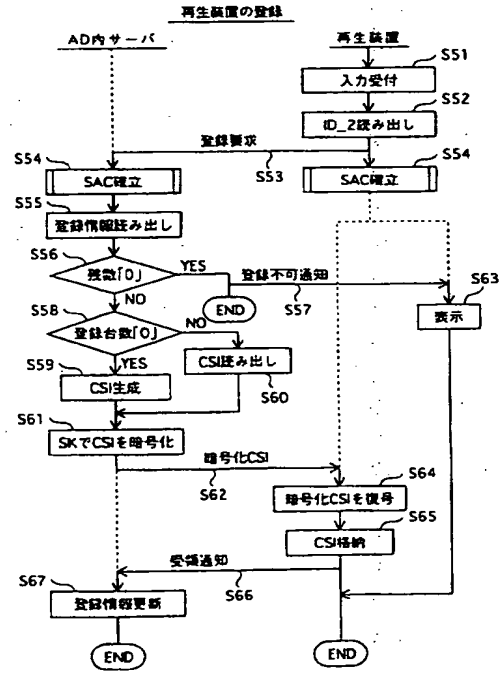
【図７】


SAC
機器A
機器B
公開鍵証明書読み出し
S11
Cert_A
S12
署名検証
S13
成功
S14
NO
YES
CRL読み出し
S15
CRLに登録有
S16
YES
NO
公開鍵証明書読み出し
S17
B2
Cert_B
S18
署名検証
S19
成功
S20
NO
YES
CRL読み出し
S21
CRLに登録有
S22
YES
NO
A2
乱数Cha_B生成
S23
Cha_B
S24
Cha_B||CSI生成
S25
署名データSig_A生成
S26
Sig_A
S27
A1
B1

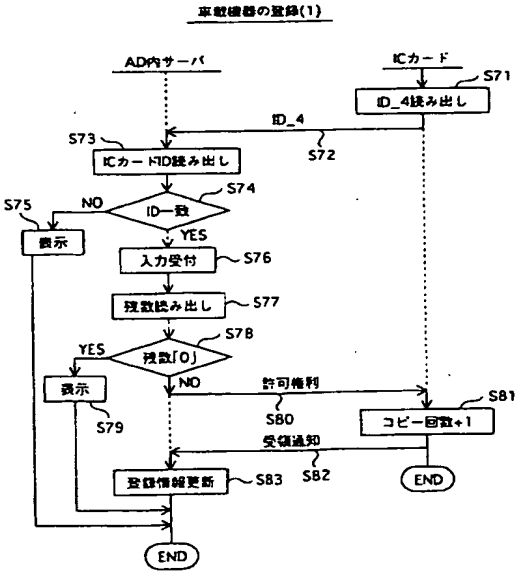
【図８】


A1
B1
署名データSig_A検証
S28
乱数Cha_A生成
S30
成功
S29
NO
B2
Cha_A
YES
S31
Cha_A||CSI生成
S32
署名データSig_B生成
S33
END
Sig_B
S34
署名データSig_B検証
S35
A2
NO
成功
S36
YES
乱数「a」生成
S37
Key_A生成
S38
END
Key_A
S39
乱数「b」生成
S40
Key_B生成
S41
Key_B
S42
Key_AB生成
S45
Key_AB生成
S43
SK生成
S46
SK生成
S44
RETURN
RETURN

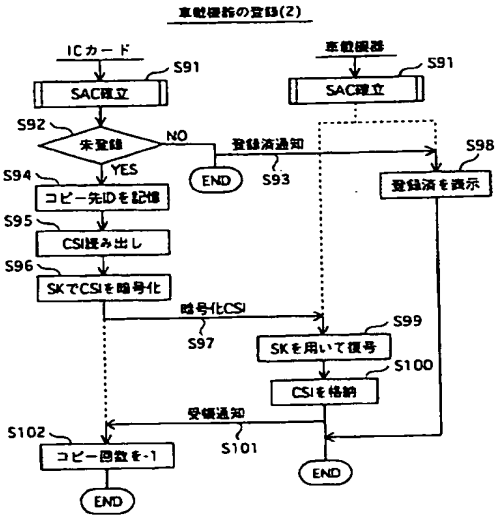
【図９】


再生装置の登録
AD内サーバ
再生装置
入力受付
S51
ID_2読み出し
S52
登録要求
S53
S54
SAC確立
SAC確立
S54
登録情報読み出し
S55
残数「0」
S56
YES
登録不可通知
S63
NO
END
S57
表示
登録台数「0」
S58
NO
YES
CSI読み出し
S60
CSI生成
S59
SKでCSIを暗号化
S61
暗号化CSI
S62
暗号化CSIを復号
S64
CSI格納
S65
受領通知
S66
登録情報更新
S67
END
END

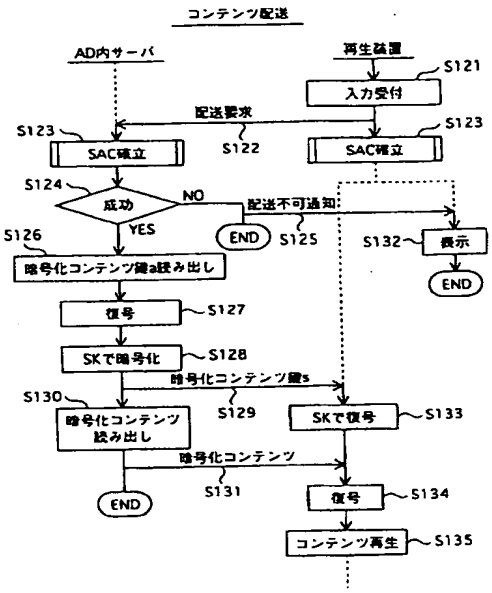
【図１０】


車載機器の登録(1)
AD内サーバ
ICカード
ID_4読み出し
S71
ID_4
S72
ICカードID読み出し
S73
ID一致
S74
NO
S75
表示
YES
入力受付
S76
残数読み出し
S77
残数「0」
S78
YES
NO
表示
S79
許可情報
S80
S81
コピー回数+1
受領通知
S82
END
登録情報更新
S83
END

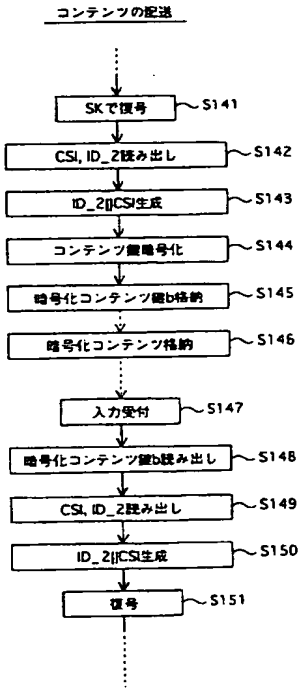
【図１１】



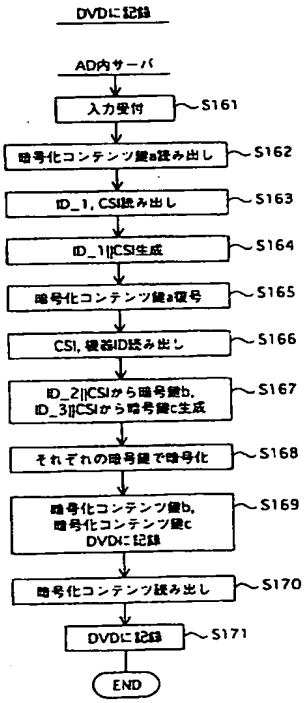

【図１２】



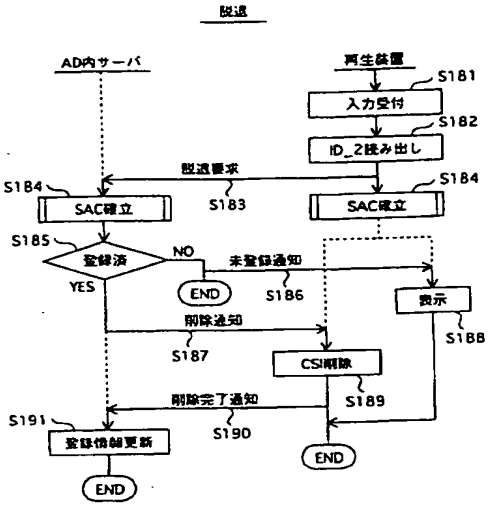

【図１３】



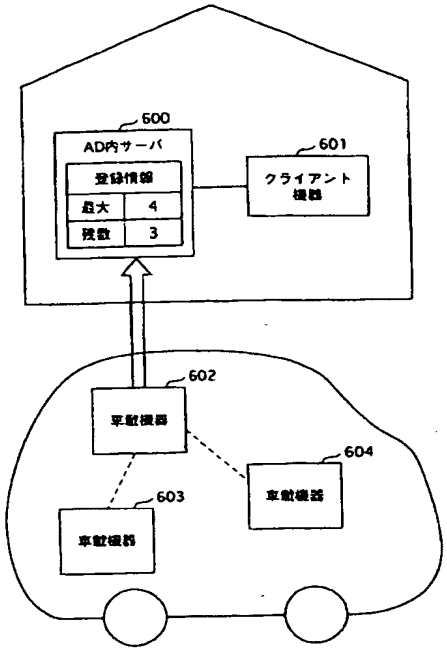

【図１４】



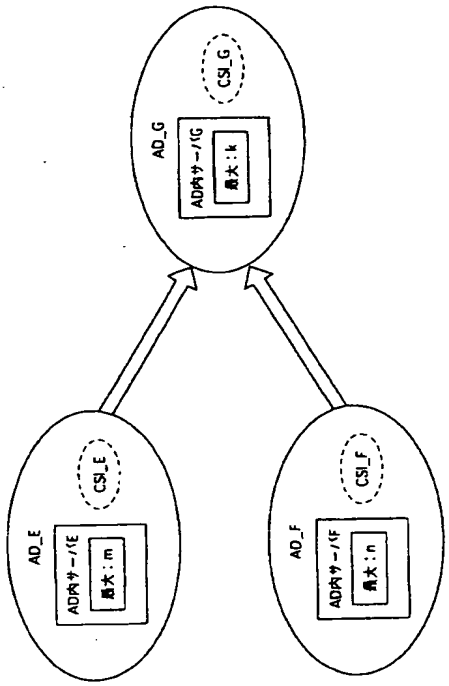
【図１５】



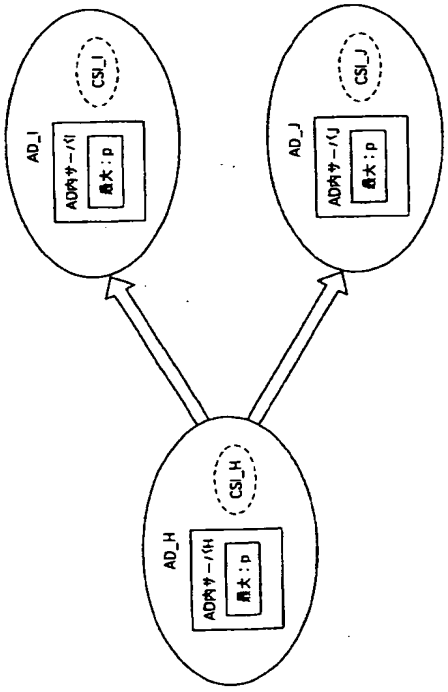

【図１６】




【図１７】




【図１８】



フロントページの続き

(72)発明者　布田　裕一
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　宮▲ざき▼　雅也
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

Ｆターム(参考) 5J104 EA17